

No. 22-1318

**IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT**

MICHAEL MUIR,
Petitioner,

v.

UNITED STATES DEPARTMENT OF HOMELAND SECURITY
AND TRANSPORTATION SECURITY ADMINISTRATION,
Respondents.

ON PETITION FOR REVIEW OF A FINAL ORDER OF THE UNITED
STATES TRANSPORTATION SECURITY ADMINISTRATION

JOINT APPENDIX

MICHAEL MUIR, *Pro Se*
19 Inglewood Lane
Bloomington, IL 61704
712-309-6121
muirone@yahoo.com
Petitioner

BRIAN M. BOYNTON
U.S. Department of Justice
Room 7527
950 Pennsylvania Ave. NW
Washington, DC 20530
202-514-0236
Counsel for Respondents

WILLIAM R. WEAVER
JENNER & BLOCK LLP
1099 New York Avenue NW
Suite 900
Washington, DC 20001
202-639-6000
wweaver@jenner.com
Counsel for Amicus Curiae

INDEX

Transportation Security Administration Certified Index of the Administrative Record	JA1
United States Department of Homeland Security Certified Index of the Administrative Record	JA22
Petition for Review, <i>Muir v. United States Department of Homeland Security</i> , No. 22-1318 (D.C. Cir. Dec. 14, 2022)	JA32
Declaration of Joseph Sebastian, <i>Muir v. United States Department of Homeland Security</i> , No. 22-1318 (D.C. Cir. Apr. 20, 2023)	JA95
Declaration of Michael Muir, <i>Muir v. United States Department of Homeland Security</i> , No. 22-1318 (D.C. Cir. May 30, 2023)	JA109
TSA-2013-0004-0001, NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication) (Mar. 26, 2013)	JA117
TSA-2013-0004-0005: Dep’t Homeland Security, <i>Advanced Imaging Technologies: Passenger Privacy Protections, Fiscal Year 2010 Report to Congress</i> (Feb. 25, 2010)	JA133
TSA-2013-0004-0163, Comments of Anonymous (Apr. 2, 2013)	JA145
TSA-2013-0004-2726, Comments of Gail Levin (June 4, 2013)	JA147
TSA-2013-0004-3545, Comments of Anonymous (June 12, 2013)	JA149
TSA-2013-0004-4233, Comments of Jay Wilson (June 25, 2013)	JA151
TSA-2013-0004-4432, Comments of Anonymous (June 26, 2013)	JA153
TSA-2013-0004-4958, Comments of Freedom to Travel USA (June 23, 2013)	JA156
TSA-2013-0004-5424, Comments of Thomas A. Burns (June 23, 2013)	JA176
TSA-2013-0004-5584-A6: United States Department of Homeland Security, <i>Privacy Impact Assessment for TSA Whole Body Imaging</i> (Dec. 18, 2015)	JA178

TSA-2013-0004-5584-A25: Homeland Security Subcommittee Hearing: Transportation Security Administration Efforts to Address IG Findings (Sept. 29, 2015), audio version available at https://www.appropriations.senate.gov/hearings/homeland-security-subcommittee-hearing-transportation-security-administration-efforts-to-address-ig-findings	JA185
TSA-2013-0004-5584-A38: United States Department of Homeland Security, <i>Privacy Impact Assessment for TSA Whole Body Imaging</i> (Jan. 2, 2008)	JA186
TSA-2013-0004-5584-A86: United States Department of Homeland Security, <i>Privacy Impact Assessment Update for TSA Advanced Imaging Technology</i> (Jan. 25, 2011).....	JA195
Defendant’s Motion to Dismiss Plaintiff’s Complaint and Memorandum of Law in Support <i>Muir v. L3Harris Technologies, Inc.</i> , No. 2:19-cv-05887 (D. Ariz. Jan. 29, 2020), ECF No. 14	JA206
Defendant’s Reply in Support of its Motion to Dismiss Plaintiff’s Complaint, <i>Muir v. L3Harris Technologies, Inc.</i> , No. 2:19-cv-05887 (D. Ariz. Mar. 20, 2020), ECF No. 19	JA238
Joint Motion for Leave to Intervene of L3Harris Technologies, Inc. and Leidos, Inc., <i>Muir v. United States Department of Homeland Security</i> , No. 22-1318 (D.C. Cir. Dec. 14, 2022)	JA251
Office of Management and Budget Memorandum for the Heads of Executive Departments and Agencies, M-24-10 (Mar. 28, 2024).....	JA276
<i>DHS Prize Competition 16-01: Passenger Screening Algorithm Challenge</i> , https://www.dhs.gov/science-and-technology/dhs-prize-competition-16-01 (last updated Aug. 1, 2024).....	JA310
DHS AI Use Case Inventory (Dec. 16, 2024 update), native version available at https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.dhs.gov%2Fsites%2Fdefault%2Ffiles%2F2024-12%2F24_1216_ocio_2024-dhs-ai-use-case-inventory_1.xlsx&wdOrigin=BROWSELINK	JA312

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

MICHAEL MUIR,

Petitioner,

v.

UNITED STATES DEPARTMENT OF HOMELAND
SECURITY and TRANSPORTATION SECURITY
ADMINISTRATION,

Respondents.

No. 22-1318

**CERTIFIED INDEX TO THE ADMINISTRATIVE
RECORD**

Pursuant to Rule 17 of the Federal Rules of Appellate Procedure, respondent Transportation Security Administration (“TSA”) hereby certifies that the material listed and described in the attached pages constitutes the administrative record relevant to this petition for review of TSA’s rulemaking regarding passenger screening using Advanced Imaging Technology (“AIT”).

Dated: May 3, 2023



Marc Pilcher
Assistant Chief Counsel for
Federal Court Litigation
Office of Chief Counsel
Transportation Security
Administration

Part I: Materials From Public Rulemaking Docket
 (available at <https://www.regulations.gov/docket?D=TSA-2013-0004>)

Description	Docket ID No.
TSA.gov webpage entitled “AIT: Safety,” dated December 22, 2012	0003
Presidential Memorandum Regarding December 25, 2009 Attempted Terrorist Attack, dated January 7, 2010	0004
TSA Fiscal Year 2010 Report to Congress, entitled “Advanced Imaging Technologies: Passenger Privacy Protections,” dated February 25, 2010	0005
TSA.gov webpage entitled “AIT: How it Works,” dated January 14, 2010	0006
FDA.gov webpage entitled “Radiation-Emitting Products – Products for Security Screening of People,” dated November 15, 2011	0007
TSA.gov webpage entitled “AIT: How it Works,” dated January 14, 2013	0008
TSA Blog Post entitled “Rapiscan Backscatter Contract Terminated – Units to be Removed,” dated January 18, 2013	0009
Privacy Impact Assessment Update for TSA Advanced Imaging Technology, January 25, 2011	0010
TSA.gov webpage entitled “AIT: How it Works,”(capturing AIT Signs), dated January 14, 2010	0011
TSA.gov webpage, entitled “AIT: Safety,” dated December 22, 2012	0012
2005 Institute of Electrical and Electronics Engineers, Inc. Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields (IEEE Std. C95.1™-2005)	0013

Description	Docket ID No.
International Commission on Non-Ionizing Radiation Protection Guidelines for Limiting Exposure to Time-Varying Electric, Magnetic, and Electromagnetic Fields, Health Physics 74(4); 494-522, published April 1998	0014
Federal Communications Commission, Office of Engineering & Technology Bulletin 65, “Evaluating Compliance with FCC Guidelines for Human Exposure to Radio frequency Electromagnetic Fields,” dated August 1997	0015
Health Canada Safety Code 6, “Limits of Human Exposure to Radiofrequency Electromagnetic Energy in the Frequency Range from 3kHz to 300 GHz,” (includes RSS-102 Issue 3 for Canada), dated 2009	0015
FDA.gov webpage entitled “Radiation-Emitting Products – Products for Security Screening of People,” dated November 15, 2011	0016
TSA.gov webpage entitled “AIT: Safety,” dated December 22, 2012	0017
Department of Homeland Security, Office of Inspector General, “Transportation Security Administration’s Use of Backscatter Units,” OIG-12-38, dated February 2012	0018
HPS Fact Sheet: Radiation Exposure from Medical Exams and Procedures, dated January 2010	0019
Federal Aviation Administration, “What Aircrews Should Know About Their Occupational Exposure to Ionizing Radiation,” DOT-FAA-AM-03-1, dated October 2003	0020
World Health Organization webpage entitled “What is Ionizing Radiation”, dated August 16, 2012	0021
European Union Scientific Committee on Emerging and Newly Identified Health Risks (SCENIHR), Health effects of security scanners for passenger screening (based on X-ray technology), dated April 26, 2012	0022

Description	Docket ID No.
TSA.gov webpage entitled “AIT: Safety,” dated December 22, 2012 (featuring link to U.S. Army Public Health Command independent security report)	0023
TSA.gov webpage collecting U.S. Army Public Health Command Radiation Surveys of General Use Backscatter X-ray Advanced Imaging Technology and Cabinet X-ray Systems, dated January 27, 2013	0023
TSA.gov webpage entitled “AIT: More Information,” dated January 17, 2013	0024
TSA.gov webpage entitled “Advanced Imaging Technology (AIT) Traveler’s Guide”, dated March 15, 201320130315	0024
TSA Blog post entitled “Opt Out Turns Into Opt In,” dated November 17, 2011	0024
TSA.gov webpage entitled “AIT: How it Works,” dated January 14, 2010	0025
TSA.gov webpage entitled “Traveling with Children,” dated February 21, 2013	0026
TSA.gov webpage entitled “AIT: Frequently Asked Questions,” dated February 22, 2013	0027
Remarks of TSA Administrator John S. Pistole, Homeland Security Policy Institute, George Washington University, November 10, 2011	0028
TSA Blog post entitled “TSA Week In Review: Non Metallic Martial Arts Weapon Found with Body Scanner,” December 30, 2011	0029
TSA Blog post entitled “Loaded .380 Found Strapped To Passenger’s Ankle at DTW With Body Scanner,” December 13, 2011	0030
TSA Blog post entitled “Advanced Imaging Off To a Great Start,” April 20, 2010, and “Advanced Imaging Technology – Yes, It’s Worth It,” March 31, 2010	0031

Description	Docket ID No.
TSA Blog post entitled “TSA Week in Review: Plastic Dagger Found With Body Scanner,” May 4, 2012	0032
TSA Blog post entitled “TSA Week in Review: Comb Dagger Discovered With Body Scanner, 28 Loaded Guns, and More,” August 17, 2012	0033
<i>Passenger Screening Using AIT</i> – Notice of Proposed Rulemaking – Initial Regulatory Impact Analysis	0035
<i>Passenger Screening Using AIT</i> – Notice of Proposed Rulemaking – Initial Regulatory Impact Analysis - Corrected Version	0035
Comments received regarding <i>Passenger Screening Using AIT</i> Notice of Proposed Rulemaking received March 28, 2015 through June 24, 2015 ¹	0036-5581
<i>Passenger Screening Using AIT</i> – Final Rule – Final Economic Analyses (Regulatory Impact Analysis & Final Regulatory Flexibility Analysis), dated February 18, 2016	5583
Presidential Memorandum Regarding December 25, 2009 Attempted Terrorist Attack, dated January 7, 2010	5584-A2
Senate Report No. 110-396 on DHS Appropriations Bill for FY 2009, dated June 23, 2008	5584-A3
RAND Corporation Paper, “Understanding Role of Deterrence in Counterterrorism Security,” Andrew R. Morral & Brian A. Jackson, published 2009	5584-A4
White House OMB, Circular A-4, Regulatory Analysis, dated September 17, 2003	5584-A5
Privacy Impact Assessment Update for TSA Advanced Imaging Technology, December 18, 2015	5584-A6

¹ Comments can be accessed in full at the docket for this rulemaking, available at

<https://www.regulations.gov/docketBrowser?rpp=25&so=DESC&sb=commentDueDate&po=0&dct=PS&D=TSA-2013-0004>

Description	Docket ID No.
TSA.gov webpages entitled “Disabilities & Medical Conditions,” dated February 26, 2016, and “Traveling with Children”	5584-A7
TSA.gov webpage entitled “TSA Pre✓®,” dated February 26, 2016	5584-A8
TSA Report to Congress entitled “Detection Equipment at Airport Screening Checkpoints” and associated correspondence, dated August 9, 2005	5584-A9
Remarks of TSA Administrator John S. Pistole at Airports Council Intl-North America, dated August 14, 2013	5584-A10
FBO.gov TSA Solicitation for Imaging Technology Systems, Solicitation No. HSTS04-08-R-CT2056, dated February 26, 2012	5584-A11
DHS.gov webpage entitled “Privacy Documents for the Transportation Security Administration (TSA),” dated February 26, 2016	5584-A12
Privacy Impact Assessment Update for TSA Advanced Imaging Technology, January 25, 2011	5584-A13
DHS-TSA Fiscal Year 2010 Report to Congress on Advanced Imaging Technologies: Passenger Privacy Protection, dated February 25, 2010	5584-A14
TSA.gov webpage entitled “Contact,” dated December 23, 2015	5584-A15
TSA.gov webpage entitled “Passenger Support – Civil Rights,” dated February 26, 2016	5584-A16
GAO Testimony Before House Committee on Oversight and Government Reform, “Aviation Security: Vulnerabilities Exposed Through Covert Testing of TSA’s Passenger Screening Process” (GAO-08-48T), dated November 15, 2007	5584-A17

Description	Docket ID No.
GAO Testimony Before House Committee on Homeland Security, Subcommittee on Transportation Security and Infrastructure Protection, “TSA Is Increasing Procurement and Deployment of the Advanced Imaging Technology, but Challenges to This Effort and Other Areas of Aviation Security Remain” (GAO-10-484T), dated March 17, 2010	5584-A18
CNS News article, “U.S. Paid for Full-Body Scanners at Nigeria’s Four International Airports in 2007,” dated January 6, 2010	5584-A19
Airbus.com webpage entitled “A380 Dimensions & Key Data,” Accessed Aug. 12, 2015	5584-A20
How Stuff Works article, “How Millimeter Wave Scanners Work,” dated February 26, 2016	5584-A21
European Commission Press Release, “Aviation Security: Commission adopts new rules on the use of security scanners at European airports,” dated November 11, 2014	5584-A22
GAO Report to Congressional Requesters, “Advanced Imaging Technology: TSA Needs Additional Information before Procuring Next-Generation Systems” (GAO-14-357), dated March 31, 2014	5584-A23
Statement of Jeh Johnson, Secretary DHS, on Inspector General Findings On TSA Security Screening, dated June 1, 2015	5584-A24
Testimony of Peter Neffenger, Administrator, TSA, before the S. Comm. on Appropriations, Subcomm. on Homeland Security, “TSA efforts to address OIG findings,” dated September 29, 2015	5584-A25
TSA.gov webpage entitled “Freedom of Information Act,” dated February 26, 2016	5584-A26
Department of Homeland Security, Office of Inspector General Report: Transportation Security Administration’s Use of Backscatter Units (OIG-12-38), dated February 2012	5584-A27

Description	Docket ID No.
Report of American Association of Physicists in Medicine (AAPM) Task Group 217, “Radiation Dose from Airport Scanners,” dated June 2013	5584-A28
The National Academies Press, “Airport Passenger Screening Using Backscatter X-Ray Machines: Compliance with Standards,” dated 2015	5585-A2
Stanford Health Care webpage entitled “Skin Cancer,” dated February 26, 2016	5585-A3
FDA webpage entitled “Products for Security Screening of People,” dated August 26, 2015	5585-A4
European Union Scientific Committee on Emerging and Newly Identified Health Risks (SCENIHR), Health effects of security scanners for passenger screening (based on X-ray technology), dated April 26, 2012	5585-A5
DHS Science and Technology Directorate, “Compilation of Emission Safety Reports on the L3 Communications, Inc. ProVision 100 Active Millimeter Wave Advanced Imaging Technology (AIT) System,” dated September 1, 2012	5585-A6
TSA.gov webpage entitled “Travel Tips,” dated February 26, 2016	5585-A7
TSA.gov webpage entitled “Frequently Asked Questions,” dated February 26, 2016	5585-A8
TSA.gov webpage entitled “Traveling With Children” and “Screening for Passengers 75 and Older”	5585-A9
TSA.gov webpage entitled “Passenger Support – Screening Assistance and Passenger Support Specialists,” dated February 26, 2016	5585-A10
TSA.gov webpage entitled “Security Screening,” dated February 26, 2016	5585-A11
TSA.gov webpage entitled “Disabilities and Medical Conditions”	5585-A12

Description	Docket ID No.
TSA.gov webpage entitled “Security Screening” and “Disabilities and Medical Conditions”	5585-A13
Australian Department of Infrastructure and Transport, “Optimal Technologies Proof of Concept Trial Report” dated February 28, 2012	5585-A14
Department of Transportation, Memorandum re. Revised Departmental Guidance on Valuation of Travel Time in Economic Analysis, dated September 28, 2011	5585-A15
Garrick Blalock, Vrinda Kadiyali, & Daniel H. Simon, “The Impact of Post 9/11 Airport Security Measures on the Demand for Air Travel,” Cornell Univ. Dyson Sch. of Econ., dated April 30, 2007	5585-A16
Department of Transportation, Office of the Assistant Secretary for Research & Technology, Bureau of Transportation Statistics, Air Carrier Statistics database (T-100 data bank)	5585-A17
Department of Transportation, Office of the Assistant Secretary for Research & Technology, Bureau of Transportation Statistics, T-100 Domestic Segment (All Carriers)	5585-A18
Department of Transportation, Office of the Assistant Secretary for Research & Technology, Bureau of Transportation Statistics, T-100 Domestic Segment (All Carriers)	5585-A19
Airbus Industries webpage providing Dimensions & Key Data for A380 Aircraft, dated August 12, 2015	5585-A20
Airbus Industries press release providing aircraft list prices for 2015, dated January 13, 2015	5585-A21
Boeing Commercial webpage providing Technical Characteristics for 777-200 Aircraft	5585-A22
Boeing Commercial webpage providing Commercial Airplane Prices for 2014 and 2015	5585-A23
Boeing Commercial webpage providing Technical Characteristics for 737-700 Aircraft	5585-A24

Description	Docket ID No.
Boeing Commercial webpage providing Technical Characteristics for 737-800 Aircraft	5585-A25
Airbus Industries webpage providing Dimensions & Key Data for A320 Aircraft, dated August 12, 2015	5585-A26
U.S. Department of Transportation 2013 Guidance on Treatment of the Economic Value of a Statistical Life in U.S. Department of Transportation Analyses	5585-A27
SmithAmundsen Aerospace Alert entitled “Colgan Air Crash Clean Up,” dated March 20, 2013	5585-A28

Part II: Additional Administrative Record Materials
(Additional material also considered by agency but not incorporated into
public rulemaking docket because it post-dates the rulemaking, was
copyrighted and proprietary, For Official Use Only, or Sensitive
Security Information)

Description	Date
Nat'l Research Council Report, "Airline Passenger Security Screening: New Technologies & Implementation Issues" (NMAB-482-1) (copyrighted material) .	June 1, 1996
Am. Nat'l Standards Inst., Inc., report designated ANSI/HPS N43.17-2002, "Radiation Safety for Personnel Security Screening Systems Using X- Rays" (copyrighted material published by Health Physics Society) (copyrighted material) .	Apr. 3, 2002
Nat'l Council on Radiation Prot. & Measurements, Commentary No. 16, "Screening of Humans for Security Purposes Using Ionizing Radiation Scanning Systems" (copyrighted material available through http://www.ncrponline.org/) .	Dec. 15, 2003
Inst. of Electrical & Electronics Eng'rs (IEEE), Standards Coordinating Comm. 39, "IEEE Recommended Practice for Radio Frequency Safety Programs, 3 kHz to 300 GHz" (IEEE Std C95.7™-2005) (copyrighted material) .	Mar. 22, 2006
Am. Nat'l Standards Inst., "Radiation Safety for Personnel Security Screening Systems Using X-Ray or Gamma Radiation" (ANSI/HPS N43.17-2009) (copyrighted material published by Health Physics Society and available through http://hps.org/hpssc/) .	Aug. 1, 2009
L3 Operations Manual for AIT-ATR (this document contains proprietary information) .	Aug. 16, 2010
TSA, Office of Intelligence, "Civil Aviation Threat Assessment" (2008) (this material is For Official Use Only) .	Mar. 20, 2008

Description	Date
TSA, Office of Intelligence, “Civil Aviation Threat Assessment” (2011) (this material is For Official Use Only).	Oct. 12, 2011
Action Memo regarding Approval & Implementation of New Torso Pat-down Procedures (this document contains Sensitive Security Information (SSI) within the meaning of 49 C.F.R. parts 15 and 1520).	Dec. 21, 2004
DHS-OIG Report 06-10 – Review of TSA’s Use of Pat-downs in Screening Procedures (TSA- 050901-008) (this document contains SSI).	Nov. 1, 2005
TSA Security Screening Checkpoint Standard Operating Procedures, Revision 8 (this document constitutes SSI in its entirety).	May 28, 2008
TSA Procurement Specification for Whole Body Imager Devices for Checkpoint Operations, Version 1.02 (this document contains SSI).	Sept. 23, 2008
Whole Body Imager Standard Operating Procedures issued by TSA (this document constitutes SSI in its entirety).	May 19, 2009
TSA brief to the Homeland Security Council titled “Imaging Technology Program” (this document contains SSI).	Aug. 7, 2009
TSA Transportation Security Lab (TSIF) Report – Threat Mitigation Experiment for Rapiscan Secure 1000® and L3 ProVision Advanced Imaging Technology (AIT) (this document constitutes SSI in its entirety).	Sept. 1, 2009
TSA “Systems Planning and Evaluation: Concept of Operations, Advanced Imaging Technology Systems” document (this document contains SSI).	Sept. 2, 2009
Excerpts from DHS Acquisition Review Board Presentation for Passenger Screening Program (this document contains SSI).	Sept. 8, 2009
TSA Procurement Specification for Advanced Imaging Technology (AIT) for Checkpoint Operations, version 2.1 (this document contains SSI).	Sept. 10, 2009

Description	Date
TSA Procurement Specification for Advanced Imaging Technology (AIT) for Checkpoint Operations, version 2.11 (this document contains SSI).	Sept. 30, 2009
Information Memo from Robin E. Kane, Assistant Adm'r, TSA, to Domenico C. Cipicchio, Assistant Adm'r, TSA, regarding "Notification To Add the Rapiscan Secure 1000 DV Advanced Imaging Technology to the Qualified Products List" (this document contains SSI).	Oct. 6, 2009
Information Memo from Robin E. Kane, Assistant Adm'r, TSA, to Domenico C. Cipicchio, Assistant Adm'r, TSA, regarding "Notification To Add the L-3 ProVision 100b Advanced Imaging technology to the Qualified Products List" (this document contains SSI).	Oct. 7, 2009
Description of Pat-down procedures under consideration (this document contains SSI).	Jan. 1, 2010
Pat-down Working Group Depiction of Proposed Pat-down Options following Flight 253 Attempt (this document contains SSI).	Jan. 1, 2010
Action Memo from Robin Kane and Lee Kair, Assistant Adm'rs, TSA, to Gale D. Rossides, Acting Adm'r, TSA, regarding "Notification of Completion of the AIT Pilot Phase and Request To Move All Installed Units to the Primary Screening Position" (this document contains SSI).	Jan. 3, 2010
Proposed Action Memo regarding Passenger Screening - Enhanced Resolution of Individuals (this document contains SSI).	Jan. 13, 2010
TSA Letter and attached Request for Deviation (RFD-002 AIT Rev. 1, dated Feb. 4, 2010) to install and test software modifying aspects of Rapiscan Secure 1000 SP (Rapiscan AIT) functionality (this document contains SSI).	Feb. 4, 2010
DHS TSL Quick Look Report for Rapiscan AIT, regarding Verification of Upgrade to Software Version 03.04.01 (this document contains SSI).	Feb. 18, 2010

Description	Date
TSA Engineering Change Proposal (ECP) issued to Rapiscan Systems, regarding change to Master Configuration Item Listing for software for Rapiscan AIT (this document contains SSI).	Feb. 23, 2010
TSA Procurement Specification for Advanced Imaging Technology (AIT) for Checkpoint Operations, version 2.11 (this document contains SSI).	Mar. 4, 2010
TSA ATR Operational Testing & Evaluation Weekly Data Report (this document contains SSI).	Mar. 22, 2010
TSA System Evaluation Report: Advanced Imaging Technology (AIT) for Rapiscan Secure 1000-Dual View (DV) (this document constitutes SSI in its entirety).	Mar. 26, 2010
TSA System Evaluation Report: Advanced Imaging Technology (AIT), for L3 Communications ProVision 100 (this document constitutes SSI in its entirety).	Mar. 26, 2010
Action Memo regarding Passenger Screening – Enhanced Resolution of Individuals (this document contains SSI).	Apr. 6, 2010
OSO Communication – Additional Screening Procedures Regarding AIT Opt-out (this document contains SSI).	Apr. 29, 2010
AIT-ATR Functional Requirements Document (this document contains SSI).	May 3, 2010
TSA report titled “Advanced Imaging Technology ‘Finds’/Incidents (Jan. - May 2010)” (this document constitutes SSI in its entirety).	May 23, 2010
Observations Regarding Sensitive Area Searches During Operational Testing & Evaluation Period (this document contains SSI).	June 1, 2010
International AIT Summit Presentation (this document contains SSI).	June 1, 2010
TSA Office of Intelligence’s Civil Aviation Threat Assessment 2010 (this document is marked For Official Use Only and contains SSI).	June 1, 2010

Description	Date
Action Memo Regarding Removing Hand-held Metal Detection From Standard Screening (this document contains SSI).	June 2, 2010
Action Memo regarding Sensitive Area Private Searches (this document contains SSI).	June 2, 2010
TSIF Test Report: Assessment of Passenger Checkpoint Security Screening Countermeasures against Northwest Airlines Flight 253-Type Threats (this document constitutes SSI in its entirety).	June 11, 2010
TSA Office of Security Technology, Statement of Work for AIT-ATR for Checkpoint Operations (this document contains SSI).	June 21, 2010
Estimate of Standard Pat-down Frequency (this document contains SSI).	June 30, 2010
Flight 253 IPT Briefing– SPD/RPD Evaluation (this document contains SSI).	July 8, 2010
Action Memo regarding Request to Proceed with Evaluation of Proposed Passenger Screening Procedures (this document contains SSI).	Aug. 9, 2010
TSIF Test Report: Comparison Between AIT Sliding & Standard Pat-down (this document contains SSI).	Aug. 13, 2010
Presentation to Secretary Napolitano re Proposed Standard & Resolution Pat-downs (this document contains SSI).	Aug. 16, 2010
AIT-ATR Qualification Plan (this document contains SSI).	Aug. 16, 2010
Pat-down Pilot Program Standard Operating Procedures (this document constitutes SSI in its entirety).	Aug. 16, 2010
Resolution Pat-down Standard Operating Procedures, version 1 (this document constitutes SSI in its entirety).	Sept. 17, 2010
Screening Checkpoint Standard Operating Procedures, Revision 9 (this document constitutes SSI in its entirety).	Sept. 17, 2010

Description	Date
TSIF Advanced Imaging Technology (AIT) System Image Characterization – Results Summary (this document constitutes SSI in its entirety).	Sept. 23, 2010
Operational Requirements Document for AIT System for Checkpoint Operations (this document contains SSI).	Sept. 28, 2010
Functional Requirements Document for AIT System with ATR for Checkpoint Operations (this document contains SSI).	Sept. 30, 2010
Presentation of AIT Incidents & Finds, June-Sept. 2010 (this document contains SSI).	Oct. 2010
Adm'r's Daily Intelligence Briefing – Excerpts re Threat Assessment (this document contains SSI).	Oct. 1, 2010
Summary of Rapiscan IO Performance during Operational Testing & Evaluation Period (this document contains SSI).	Oct. 10, 2010
Summary of L3 IO Performance during Operational Testing & Evaluation Period (this document contains SSI).	Oct. 15, 2010
Testing Plan for Field Evaluation of Image Operator vs. ATR Capabilities (this document contains SSI).	Nov. 4, 2010
Decision Memo regarding changes to Screening Checkpoint Standard Operating Procedures, Revision 9, for Opposite Gender Screening/Screening of Children Pat-down Mitigation Strategies (this document contains SSI).	Nov. 12, 2010
Rapiscan ATR Qualification Data Package (this document contains SSI).	Nov. 12, 2010
TSIF Report – L3 AIT Alternate Stances (with and without ATR) (this document constitutes SSI in its entirety).	Dec. 9, 2010
TSA Screening Checkpoint Standard Operating Procedures, Revision 9, Change 1 (this document constitutes SSI in its entirety).	Dec. 10, 2010
Presentation re Field Evaluation of IO vs. ATR Capabilities (this document contains SSI).	Dec. 20, 2010

Description	Date
Action Memo re Deficient Requirements re L3 AIT-ATR Qualification Testing (this document contains SSI).	Jan. 31, 2011
TSIF Report – L3 AIT ATR Anomaly Consistency Assessment (this document constitutes SSI in its entirety).	Feb. 8, 2011
AIT-ATR Operational Test Plan for OT&E of ATR (this document contains SSI).	Feb. 24, 2011
Resolution Pat-down SOP Rev. 1, Change 2 (this document constitutes SSI in its entirety).	Mar. 8, 2011
TSA Screening Checkpoint Standard Operating Procedures, Revision 9, Change 2 (this document constitutes SSI in its entirety).	Mar. 8, 2011
Presentation of AIT Incidents & Finds, Jan.-Mar. 2011 (this document contains SSI).	Apr. 2011
System Evaluation Report, L3 AIT-ATR (this document constitutes SSI in its entirety).	May 6, 2011
DHS Science & Technology Directorate, Transportation Security Lab (TSL) Final Report, Lab Qualification Test, L3 ProVision 100 -- Advanced Imaging Technology with Automatic Target Recognition (AIT-ATR) (this document constitutes SSI in its entirety).	May 9, 2011
Action Memo re Threat Testing During QT&E for L3 AIT-ATR (this document contains SSI).	June 6, 2011
Action Memo re Remedying Deficiencies in L3 AIT-ATR (this document contains SSI).	June 7, 2011
DHS Acquisition Review Board Presentation – Automated Target Recognition (this document contains SSI).	June 13, 2011
DHS DOT&E Letter of Assessment re AIT-ATR Follow-on Operational Test & Evaluation (this document contains SSI).	June 22, 2011
Advanced Imaging Technology - Automated Target Recognition Briefing (this document contains SSI).	July 2011

Description	Date
L-3 ProVision™ Standard Operating Procedures for AIT with ATR (this document constitutes SSI in its entirety).	July 13, 2011
TSIF Report – AIT Image Characterizations of Flight 253 Simulant Test Articles (this document constitutes SSI in its entirety)	July 17, 2011
TSA Screening Checkpoint Standard Operating Procedures (rev. 9, chg. 3) (this document constitutes SSI in its entirety).	Aug. 25, 2011
Action Memo—Criteria for Inclusion in Fall 2011 Risk-Based Security Pilot 2011 (this document constitutes SSI in its entirety).	Sept. 30, 2011
Screening Checkpoint Standard Operating Procedures, Revision 9, Change 4 (this document constitutes SSI in its entirety).	Feb. 13, 2012
Action Memo re Approval to proceed with TSA Pre✓™ Implementation (this document constitutes SSI in its entirety).	Feb. 16, 2012
Photograph (this document constitutes SSI in its entirety).	(undated)
TSA Screening Checkpoint SOP (rev. 9, chg. 5) (this document constitutes SSI in its entirety).	July 9, 2012
Information Memo re Managed Inclusion Proof of Concept Underway (this document constitutes SSI in its entirety).	Dec. 14, 2012
Action Memo re Approval to Adjust Managed Inclusion Procedures for Continued Field Assessment (this document constitutes SSI in its entirety).	Jan. 18, 2013
Action Memo – Removal of Advanced Imaging Technology Systems (AIT) without Automated Target Recognition (ATR) in compliance with Federal Aviation Administration (FAA) Modernization & Reform Act (this document contains SSI).	Jan. 21, 2013

Description	Date
Risk-Based Security (RBS)—TSA Pre✓™ SOP (rev. 1, chg. 2) (this document constitutes SSI in its entirety) .	Feb. 15, 2013
Security Countermeasures Branch (SCB) AITs in TSA Pre✓™ Lanes Findings, Version 40 (this document contains SSI) .	Mar. 2014
Concept of Operations for Enhanced Selectee Screening Procedures (this document contains SSI) .	June 18, 2015
Screening Checkpoint SOP, Revision 11 (this document constitutes SSI in its entirety) .	Oct. 5, 2015
AIT Resolution Phase II Operational Assessment SOP (this document contains SSI) .	Oct. 21, 2015
Information Memo – Actions Taken To Improve the Selectee Screening Process (this document contains SSI) .	Oct. 30, 2015
Action Memo – Enhancement of Selectee Screening Process (CONOPS) (this document contains SSI) .	Nov. 10, 2015
Action Memo – Enhanced Selectee Screening Procedures for Nationwide Implementation (this document contains SSI) .	Dec. 7, 2015
Action Memo – Enhanced AIT Alarm Resolution Procedures (this document contains SSI) .	Dec. 7, 2015
OSO Communications – Release of Enhanced Procedures for Selectee Screening and Advanced Imaging Technology Alarm Resolution (this document contains SSI) .	Dec. 8, 2015
Screening Checkpoint SOP, Revision 11, Change 1 (Chapters 2 and 10) (this document constitutes SSI in its entirety) .	Dec. 8, 2015
Screening Checkpoint SOP Summary of Changes, Revision 11 (this document constitutes SSI in its entirety) .	Dec. 8, 2015
Information Memo – Enhanced Selectee Screening Procedures for Nationwide Implementation (this document contains SSI) .	Jan. 4, 2016
Mission Essentials: Threat Mitigation training presentation (this document contains SSI) .	Jan. 16, 2016

Description	Date
TSA Tiger Team Update to H. and S. Appropriations Comm. (this document contains SSI).	Jan. 29, 2016
L-3 Communications Security & Detection Systems, AIT ATR QPL (this document contains SSI).	(undated)
Checkpoint and Specialized Security Screening SOP (this document is SSI in its entirety).	Nov. 21, 2022
Declaration of Joseph Sebastian, Assistant Federal Security Director – Generalist, St. Petersburg/Clearwater International Airport, Clearwater, Florida	Apr. 20, 2023

[Index omits classified documents that are part of the administrative record but were not included in the public docket because of their classification status]

CERTIFICATE OF SERVICE

I hereby certify that on May 3, 2023, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit by using the appellate CM/ECF system. Service on Amicus for Petitioner will be completed using the appellate CM/ECF system. Service on Petitioner will be completed by mailing a copy of the same to the name and address below:

Michael Muir
19 Inglewood Lane
Bloomington, IL 61704

/s/ Joshua Waldman

JOSHUA WALDMAN
Counsel For Respondents

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

MICHAEL MUIR,

Petitioner,

v.

UNITED STATES DEPARTMENT OF HOMELAND
SECURITY and TRANSPORTATION SECURITY
ADMINISTRATION,

Respondents.

No. 22-1318

CERTIFIED INDEX OF THE ADMINISTRATIVE RECORD

Pursuant to Rule 17 of the Federal Rules of Appellate Procedure, respondent United States Department of Homeland Security (“DHS”) hereby certifies that the material listed and described in the attached pages constitutes the administrative record relevant to this petition for review of DHS’s Designation and Certification of advanced imaging technology pursuant to the SAFETY Act, 6 U.S.C. § 441 *et seq.*

Dated: May 2, 2023

LATASHA R THOMPSON
Digitally signed by
LATASHA R THOMPSON
Date: 2023.05.02
16:10:01 -04'00'

LaTasha Thompson
Director, Office of SAFETY
Act Implementation

DOCUMENT NUMBER	BATES NUMBER	DOCUMENT DESCRIPTION
1	000001- 000001	Renewal Details signed June 27, 2016
2	000002- 000029	SAFETY Act Renewal L-3 Security and Detection Systems Corporation and L-3 Communications Corporation.
3	000030- 000086	ProVision® ATD 3.10.118 Technical Overview Training, L-3 Communications Security & Detection Systems
4	000087- 000087	PV2 System Test Record used with PV2 Test Procedure 8000-21471-TP; L3 Communications
5	000088- 000298	ProVision® ATD System Technical Manual; L3 Security & Detection Systems
6	000299- 000354	L3 ProVision® ATD Software Version E3.12.xx, Operator Manual, November 2013
7	000355- 000357	Release Notes ProVision® software 3.10.118, SW P/N: 7200-22151-SW, 3.10.118, Non STORAGE, PV1, TSA
8	000358- 000376	Concept of Operations (CONOPS) Provision ATD Aviation Applications, May 2013
9	000377- 000394	Concept of Operations (CONOPS) ProVision 2 Aviation Applications, May 2013
10	000395- 000504	Installation Manual, L2 ProVision 2 - Model 1000-10002-PV, October 2013
11	000505- 000507	Release Notes ProVision® software 3.20,131, SW P/N: 7200-22955-SW, 3.20.131, PV2, TSA
12	000508- 000561	Software Version 3.20.XX International Applications OPERATOR MANUAL November 2013
13	000562- 000564	PROVISION 2 SERIAL NUMBER AND ASSEMBLY RECORD
14	000565- 000568	Provision 2 TSA System Crate Checklist
15	000569- 000570	Provision 2 (PV2) Main Assembly Quality Check
16	000571- 000572	ProVision 2 (PV2) Upper Frame Assembly Quality Check

DOCUMENT NUMBER	BATES NUMBER	DOCUMENT DESCRIPTION
17	000573- 000574	Provision 2 (PV2) Electrical Enclosure Assembly Quality Check
18	000575- 000575	System Data Sheet Failures
19	000576- 000577	Letter from EUROPEAN CIVIL AVIATION CONFERENCE dated February 20, 2014, re: ECAC Common Evaluation Process of security equipment (CEP) Security Scanners (SSc) – Test results (2013- SSc-SRT-019)
20	000578- 000579	Letter from EUROPEAN CIVIL AVIATION CONFERENCE dated December 1, 2014, re: ECAC Common Evaluation Process of security equipment (CEP) Security Scanners (SSc) – Simulator Re-Test results (2014-SSC-SRT-004)
21	000580- 000719	L3 ProVision® 2 Maintenance Manual January 2015
22	000720- 000867	Corrective Maintenance, 8100-20602-TM, Revision A3
23	000868- 000878	Product Realization Operating Procedure, Rev. G5
24	000879- 000879	Authorization to Mark, Intertek Testing Services NA, Inc.
25	000880- 000880	Summary of Results presented to: L-3 Communications Security & Detection Systems
26	000881- 000890	Software Development Operating Procedure, Rev. A0
27	000891- 000947	ProVision 2 Operator Training
28	000948- 000948	Letter dated June 23, 2015, Attention: Mr. Dan Curtis, L3 Communications Security & Detection Systems, re: TSA Qualified Technology
29	000949- 000996	ProVision 2 Test Report - Sensitive Security Information (SSI) (Password Protected)
30	000997- 001064	SER - Sensitive Security Information (SSI) (Password Protected)
31	001065- 001122	ProVision ATD Test Report - Sensitive Security Information (SSI) (Password Protected)

DOCUMENT NUMBER	BATES NUMBER	DOCUMENT DESCRIPTION
Historical Application Documents F-23-A Designation and Certification		
32	001123-001140	Combined QATT + GCD Application, Application ID #: C-HUM-BFINCHSFVIEW-1-1
33	001141-001141	F-26A - Non-Proprietary Technology Description
34	001142-001142	SAFEVIEW, INC. SAFETY ACT APPLICATION FOR SCOUT™ SYSTEMS
35	001143-001181	SAFEVIEW, INC. SAFETY ACT APPLICATION FOR SCOUT™ SYSTEMS
36	001182-001193	Section 11: Provide any risk management plan and risk analyses related to the ATT for the past three years
37	001194-001196	Section 12: Financial Information
38	001197-001199	Section 13: Prospective Data
39	001200-001201	Section 14: Product Related Spending
40	001202-001202	Document and provide all analyses/studies that establish the degree to which the ATT performs as intended
41	001203-001207	SAFETY Act Certification Letter dated December 8, 2005 to Mr. Michael Lyons, SafeView, Inc. re: Application ID #: C-CYBER-BFINCHSFVIEW-1-1
42	001208-001211	SAFETY Act Designation Letter dated December 8, 2005 to Mr. Michael Lyons, SafeView, Inc. re: Application ID #: C-CYBER-BFINCHSFVIEW-1-1
43	001212-001217	Memorandum dated November 18, 2005 from Wendy Howe, Director, Office of SAFETY Act Implementation to Dr. Charles E. McQueary, Under Secretary for Science and Technology re: SAFETY Act Application for Designation and Certification for SafeView, Inc. C-CYBER-BFINCHSFVIEW-1-1, Scout TM Systems
44	001218-001218	Exhibit A SAFEVIEW, INC. C-CYBER-BFINCHSFVIEW-1-1 – SCOUT™ SYSTEMS
Historical Application Documents F-23-A Modification Transfer		

DOCUMENT NUMBER	BATES NUMBER	DOCUMENT DESCRIPTION
45	001219-001219	SAFEVIEW, INC. APRIL 27, 2006, RFI RESPONSE (APPLICATION NO. C-CYBER-BFINCHSFVIEW-1-1)
46	001220-001222	Draft (7.11.06) - Memorandum from Mark F. Kaye to Linda Vasta re: Acquisition of Seller of a Qualified Anti-terrorism Technology (QATT)
47	001223-001223	Signed Letter dated November 3, 2006 to Mr. Michael Lyons of SafeView, Inc. re: application ID: C-CYBER-BFINCHSFVIEW-1-1 (F-26-A)
48	001224-001226	Memorandum from Mark F. Kaye to Silvia Cabrera re: Acquisition of Seller of a Qualified Anti-terrorism Technology (QATT)
49	001227-001227	Unsigned Letter dated November 3, 2006 to Mr. Michael Lyons of SafeView, Inc. re: application ID: C-CYBER-BFINCHSFVIEW-1-1 (F-26-A)
50	001228-001228	Exhibit A SAFEVIEW, INC. C-CYBER-BFINCHSFVIEW-1-1 – SCOUT™ SYSTEMS
Historical Application Documents F-23-B Designation Renewal		
51	001229-001229	Renewal details Signed October 26, 2010
52	001230-001251	SAFETY Act Renewal Application L-3 Security and Detection Systems, Inc. and L-3 Communications Corp.
53	001252-001258	Attachment 1 - PROVISION MANUFACTURING PLAN
54	001259-001325	Attachment 2 - L3 Communications Security & Detection Systems Maintenance Course Schedule
55	001326-001582	Attachment 3 - L3 Communications Safeview PRC00284 ProVision Software Documentation Version TSA3.6
56	001583-001617	Attachment 4 - L3 Communications Security & Detection Systems Operations Manual, L-3 ProVision™ SC-100 Advanced Imaging Technology, January 2010
57	001618-001660	Attachment 5 - L3 Communications Security & Detection Systems Pro Vision SC-100 User Manual

DOCUMENT NUMBER	BATES NUMBER	DOCUMENT DESCRIPTION
58	001661- 001689	Attachment 6 - L3 Communications Security & Detection Systems Service Manual, L-3 ProVision™ SC-100 Advanced Imaging Technology, January 2010
59	001690- 001702	Attachment 7 - L3 Communications Security & Detection Systems ProVision100™ Image Quality Chart Use Procedure October 2008
60	001703- 001749	Attachment 8 - L3 Communications Security & Detection Systems ProVision SC100 Test Procedure
61	001750- 001750	Attachment 9 - Letter dated November 3, 2006 to Mr. Michael Lyons of SafeView, Inc. re: application ID: C-CYBER-BFINCHSFVIEW-1-1 (F-26-A)
62	001751- 001751	Attachment 10 - Letter dated October 21, 2009 to Mr. Paul Erhard, L-3 Communications Security & Detection Systems re: Provision SC-100 TCOP TSA - Qualified Products List (QPL)
63	001752- 001752	Attachment 11 - Spreadsheet
64	001753- 001757	Attachment 12 - Spreadsheet Installed Parts Report
65	001758- 001925	Attachment 13 - UNITED STATES SECURITIES AND EXCHANGE COMMISSION, WASHINGTON, D.C. 20549, FORM 10-K ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934 for L-3 Communications Holdings, Inc. and L-3 Communications Corporation
66	001926- 001926	DISCLAIMER APPLIES TO ALL ATTACHED DOCUMENTS
67	001927- 001927	F-26-B-L-3 Security and Detection Systems Corporation and L-3 Communications Corporation Pro Vision TM Systems
68	001928- 001928	Executive Secretariat Tracking Coordination Sheet 11-0001.16 February 11, 2011
69	001929- 001930	Letter dated February 23, 2011 to Mr. Sam Gallo, VP and General Counsel, L-3 Communications Security

DOCUMENT NUMBER	BATES NUMBER	DOCUMENT DESCRIPTION
		and Detection Systems, Inc. and L-3 Communications Corporation re: Denial of SAFETY Act Certification
70	001931-001935	Letter dated February 23, 2011 to Mr. Sam Gallo, VP and General Counsel, L-3 Communications Security and Detection Systems, Inc. and L-3 Communications Corporation re: Certificate of SAFETY Act Designation
71	001936-001942	Memorandum from Bruce Davidson, Director, Office of SAFETY Act Implementation to Paul Benda, Deputy Under Secretary for Science and Technology (Acting) re: SAFETY Act Application for Renewal of Designation and Certification (F-26-B)
72	001943-001944	Contact Tracking Data Sheet dated April 21, 2011
73	001945-001947	Emails from TSL
74	001948-001949	Emails to File from Counsel
75	001950-001951	F-26-B L3 WBI and AIT RMA data 12292010
Historical Application Documents F-23-C Certification Only		
76	001952-001954	Application G-BFINCHSFVIEW-1-REN2
77	001955-001963	F-26-C ATT Details Application for SAFETY Act Certification
78	001964-001965	Attachment 1 - Denial of SAFETY Act Certification letter dated February 23, 2011 to Mr. Sam Gallo, VP and General Counsel, L-3 Communications Security and Detection Systems, Inc. and L-3 Communications Corporation
79	001966-001972	Attachment 2 - AIT TSA Systems, CDRL L023, Based on Critical Relevant Downtime Cases, July 2011
80	001973-001979	Attachment 3 - L3 Communications Security & Detection Systems Provision Manufacturing Plan
81	001980-002046	Attachment 4 - L3 Communications Security & Detection Systems Maintenance Course Schedule

DOCUMENT NUMBER	BATES NUMBER	DOCUMENT DESCRIPTION
82	002047- 002081	Attachment 5 - L3 Communications Security & Detection Systems Operations Manual L-3 ProVision™ SC-100 Advanced Imaging Technology January 2010
83	002082- 002124	Attachment 6 - L3 Communications Security & Detection Systems ProVision SC-100 User Manual
84	002125- 002153	Attachment 7 - L3 Communications Security & Detection Systems Service Manual L-3 ProVision™ SC-100 Advanced Imaging Technology January 2010
85	002154- 002166	Attachment 8 - L3 Communications Security & Detection Systems ProVision100™ Image Quality Chart Use Procedure October 2008
86	002167- 002213	Attachment 9 - L3 Communications Security & Detection Systems ProVision SC100 Test Procedure
87	002214- 002214	Attachment 10 - Letter dated October 21, 2009 to Mr. Paul Erhard, L-3 Communications Security & Detection Systems re: Provision SC-100 TCOP TSA - Qualified Products List (QPL)
88	002215- 002215	DISCLAIMER APPLIES TO ALL ATTACHED DOCUMENTS
89	002216- 002217	Certificate of Conformance granted to L-3 Communications Corporation for its ProVision TM SC-100
90	002218- 002223	Letter dated March 23, 2012 to Mr. Gregory Lopez, L-3 Communications Security and Detection Systems, Inc, and L-3 Communications Corporation re: Application ID#: (F-26-C) G-BFINCHSFVIEW-1-REN2
91	002224- 002224	Department of Homeland Security Record of Clearance and Approval re: SAFETY Act Application (F-26-C)
92	002225- 002230	Memorandum from Bruce Davidson, Director, Office of SAFETY Act Implementation to Paul Benda, Deputy Under Secretary for Science and Technology (Acting) re: SAFETY Act Application for Certification (F-26-C)

DOCUMENT NUMBER	BATES NUMBER	DOCUMENT DESCRIPTION
93	002231- 002232	Contact Tracking Data Sheet dated February 8, 2012
Historical Application Documents F-23-D Incomplete		
94	002233- 002233	Renewal Details
95	002234- 002250	SAFETY Act Renewal Application L-3 Security and Detection Systems, Inc. and L-3 Communications Corp.
96	002251- 002251	Letter dated April 29, 2016 to Ms. Marie Rej, L-3 Communications Security and Detection Systems, Inc. re: Application ID: (F-26-D) C-CYBER-BFINCHSFVIEW-1-1-REN2
SAFETY Act Signed Final Documents		
97	002252- 002252	Department of Homeland Security Record of Clearance and Approval re: SAFETY Act Application (F-26-E)
98	002253- 002259	Letter dated October 26, 2016 to Ms. Marie Rej, L-3 Communications Security and Detection Systems, Inc. re: SAFETY Act Certification Award
99	002260- 002265	Letter dated October 26, 2016 to Ms. Marie Rej, L-3 Communications Security and Detection Systems, Inc. re: Certificate of SAFETY Act Designation
100	002266- 002275	Memorandum from Bruce Davidson, Director, Office of SAFETY Act Implementation to Fr. Robert P. Griffin, Deputy Under Secretary for Science and Technology, re: SAFETY Act Application for Renewal of Designation and Certification (F-26-E)

CERTIFICATE OF SERVICE

I hereby certify that on May 3, 2023, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit by using the appellate CM/ECF system. Service on Amicus for Petitioner will be completed using the appellate CM/ECF system. Service on Petitioner will be completed by mailing a copy of the same to the name and address below:

Michael Muir
19 Inglewood Lane
Bloomington, IL 61704

/s/ Joshua Waldman

JOSHUA WALDMAN
Counsel For Respondents

UNITED STATES COURT OF APPEALS
FOR DISTRICT OF COLUMBIA CIRCUIT

DEC 14 2022

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

RECEIVED

MICHAEL MUIR,

Petitioner

V.

UNITED STATES DEPARTMENT OF
HOMELAND SECURITY; UNITED
STATES TRANSPORTATION
SECURITY ADMINISTRATION,

Respondents

22-1318

PETITION FOR REVIEW

Pursuant to 49 U.S.C. § 46110 and Rule 15 of the Federal Rules of Appellate Procedure, Michael Muir petitions the Court for a review of two inescapably-intertwined United States Department of Homeland Security (“DHS”) and United States Transportation Security Administration (“TSA”) final orders: (1) the final promulgation of 49 C.F.R. § 1540.107(d), a DHS/TSA order issued March 3, 2016, (81 FR 11363, 11405), and (2) the SAFETY Act (6 U.S.C. § 441 *et seq.*) Certification and Designation for the TSA passenger security screening advanced imaging technology (“AIT”) millimeter wave scanner portal device, a DHS order issued October 26, 2016, both of which are attached to this petition for review.

By way of background, on December 1, 2022, Petitioner, a forty-one year old United States citizen with a hidden, completely beneath-the-skin, completely human tissue qualified physical disability under 29 U.S.C. § 705(20) (which limits

his life activities and unpredictably and uncontrollably manifests serious and periodically life-threatening symptoms as a right scrotum/groin hernia) arrived at the St. Pete-Clearwater International Airport (“PIE”) in Pinellas County, Florida, approximately two hours before his scheduled flight time of 6:10 a.m. Petitioner presented at the Checkpoint and TSA personnel confirmed his identity, scanned his valid boarding pass, and authorized him to proceed to passenger screening.

But Petitioner was, solely by reason of his disability, severely inhibited from presenting for passenger security screening due to: (1) the unpredictable and uncontrollable symptom manifestation of his serious health condition and qualified physical disability at his right groin which, due to Petitioner’s medical needs, prevented a pat-down option, and (2) the configuration of the AIT in use at the Checkpoint under the SAFETY Act (6 U.S.C. § 441 *et seq.*), which, in violation of the limits of AIT passenger screening under 49 U.S.C. § 44901(l), algorithmically misidentifies Petitioner’s hernia as a threat object requiring a pat-down to resolve.

Petitioner was thereby, in violation of 29 U.S.C. § 794(a) and the Equal Protection Clause, excluded from the participation in, and denied the benefits of the TSA Checkpoint due solely to his disability, and, as a result, could not access the sterile area, board the plane, or travel as authorized by 49 U.S.C. § 40103(a)(2).

Therefore, pursuant to 5 U.S.C. § 706 and 49 U.S.C. § 46110(c), Petitioner hereby petitions the Court to:

(1) hold unlawful and set aside the final promulgation of DHS/TSA regulation 49 C.F.R. § 1540.107(d) (81 FR 11363, 11405, March 3, 2016);

(2) compel DHS/TSA to amend the final TSA AIT passenger screening regulation to include a full and fair notice with regard to the revelation of hidden physical disabilities and the use of artificial intelligence as the final decision-maker in the millimeter wave AIT passenger security screening threat assessment loop;


(3) compel DHS to amend the millimeter wave AIT device SAFETY Act Certification and Designation to reflect the “proprietary code” artificial intelligence algorithm configuration of the “QATT” AIT in use at the TSA Checkpoint;

(4) hold unlawful and set aside the October 26, 2016 DHS SAFETY Act Certification and Designation for the millimeter wave scanner AIT device in use at the TSA Checkpoint, as the configuration of the device in use by DHS/TSA is not, and cannot ever be, described by “Exhibit A” (F-26-E) of the order; and,

(5) compel DHS/TSA to engage in, under 5 U.S.C. § 551, *et seq.*, a rulemaking notice and comment period with regard to the use of artificial intelligence in the TSA Checkpoint AIT passenger security screening program.

Dated: December 13, 2022

By: MICHAEL MUIR, *PRO SE*



Michael Muir
P.O. Box 1791
Sarasota, FL 34230
(712) 309-6121
muirone@yahoo.com



FEDERAL REGISTER

Vol. 81

Thursday,

No. 42

March 3, 2016

Part II

Department of Homeland Security

Transportation Security Administration

49 CFR Part 1540

Passenger Screening Using Advanced Imaging Technology; Final Rule

11364

Federal Register / Vol. 81, No. 42 / Thursday, March 3, 2016 / Rules and Regulations

DEPARTMENT OF HOMELAND SECURITY**Transportation Security Administration****49 CFR Part 1540**

[Docket No. TSA-2013-0004]

RIN 1652-AA67

Passenger Screening Using Advanced Imaging Technology**AGENCY:** Transportation Security Administration, DHS.**ACTION:** Final rule.

SUMMARY: The Transportation Security Administration (TSA) is amending its civil aviation security regulations to specify that TSA may use advanced imaging technology (AIT) to screen individuals at security screening checkpoints. This rule is issued to comply with a decision of the U.S. Court of Appeals for the District of Columbia Circuit, which ordered TSA to engage in notice-and-comment rulemaking on the use of AIT for passenger screening.

DATES: Effective May 2, 2016.

FOR FURTHER INFORMATION CONTACT: Chawanna Carrington, Acting Passenger Screening Program Portfolio Section Lead-Checkpoint Solutions and Integration Division, Office of Security Capabilities—Transportation Security Administration, OSCCSI-PSP@tsa.dhs.gov, 571-227-2958 (phone), 571-227-1931 (fax).

SUPPLEMENTARY INFORMATION:**Availability of Rulemaking Document**

You can get an electronic copy using the Internet by—

(1) Searching the electronic Federal Docket Management System (FDMS) Web page at <http://www.regulations.gov>; or

(2) Accessing the Government Printing Office's Web page at <http://www.gpo.gov/fdsys/browse/collection.action?collectionCode=FR> to view the daily published **Federal Register** edition; or accessing the "Search the **Federal Register** by Citation" in the "Related Resources" column on the left, if you need to do a Simple or Advanced search for information, such as a type of document that crosses multiple agencies or dates.

In addition, copies are available by writing or calling the individual in the **FOR FURTHER INFORMATION CONTACT** section. Make sure to identify the docket number of this rulemaking.

Small Entity Inquiries

The Small Business Regulatory Enforcement Fairness Act (SBREFA) of

1996 requires TSA to comply with small entity requests for information and advice about compliance with statutes and regulations within TSA's jurisdiction. Any small entity that has a question regarding this document may contact the person listed in the **FOR FURTHER INFORMATION CONTACT** section. Persons can obtain further information regarding SBREFA on the Small Business Administration's Web page at <https://www.sba.gov/category/advocacy-navigation-structure/regulatory-policy/regulatory-flexibility-act/sbreffa>.

Abbreviations and Terms Used in This Document

AIT Advanced Imaging Technology
 ANSI American National Standards Institute
 APA Administrative Procedure Act
 ATR Automatic Target Recognition
 ATSA Aviation and Transportation Security Act
 CAPPS Computer-Assisted Passenger Prescreening System
 CDRH Center for Devices and Radiological Health
 CFR Code of Federal Regulations
 DHS Department of Homeland Security
 DOJ Department of Justice
 DNA Deoxyribonucleic acid
 EAJA Equal Access to Justice Act
 E.O. Executive Order
 ETD Explosives Trace Detection Devices
 FAA Federal Aviation Administration
 FDA Food and Drug Administration
 FR **Federal Register**
 GAO Government Accountability Office
 HPS Health Physics Society
 ICAO International Civil Aviation Organization
 IEEE International Electronic and Electrical Engineers
 IRFA Initial Regulatory Flexibility Analysis
 LCCE Life Cycle Cost Estimate
 NEPA National Environmental Policy Act of 1969
 NPRM Notice of Proposed Rulemaking
 OCRL/OTE Office of Civil Rights and Liberties, Ombudsman and Traveler Engagement
 OMB Office of Management and Budget
 OSC Office of Security Capabilities
 PIA Privacy Impact Assessment
 PMIS Performance Management Information System
 PMO Program Management Office
 PRA Paperwork Reduction Act
 RFA Regulatory Flexibility Act of 1996
 RIA Regulatory Impact Analysis
 SAM Screener Allocation Model
 SOP Standard Operating Procedure
 SSI Sensitive Security Information
 THz Terahertz
 TSA Transportation Security Administration
 TSL Transportation Security Laboratory
 TSO Transportation Security Officer
 UMRA Unfunded Mandates Reform Act
 U.S.C. United States Code
 WTMD Walk Through Metal Detector

Table of Contents

I. Background

- A. Summary of the Final Rule
- B. Purpose of the Final Rule
- C. Costs and Benefits
- D. Changes From the NPRM
- II. Public Comments on the NPRM and TSA Responses
 - A. Summary
 - B. Support for AIT
 - C. Opposition to AIT
 - D. TSA Authority To Use AIT
 - E. Congressional Directive To Deploy AIT
 - F. Compliance With the Administrative Procedure Act
 - G. Adherence to the Court's Decision in *EPIC v. DHS*
 - H. Fourth Amendment Issues
 - I. Other Legal Issues
 - J. Evolving Threats to Security
 - K. TSA's Layers of Security
 - L. Effectiveness of AIT Screening
 - M. Screening Measures Used in Other Countries
 - N. Laboratory and Operational Testing of AIT Equipment
 - O. Radiation Exposure
 - P. Other Health and Safety Issues
 - Q. Backscatter Technology
 - R. Millimeter Wave Technology
 - S. Concerns Regarding Privacy
 - T. Use of ATR Software
 - U. Protection of Images
 - V. Conducting a Pat-Down as an Alternative to AIT
 - W. AIT Screening Procedures at the Checkpoint
 - X. AIT Screening Procedures for Families and Individuals With Medical Issues
 - Y. Comments on the Proposed Regulatory Text
 - Z. Costs of the Proposed Rule
 - AA. Passenger Opportunity Costs
 - BB. Airport Utility Costs
 - CC. TSA Costs
 - DD. Other Costs
 - EE. Benefits of the Proposed Rule
 - FF. Other Impacts of the Proposed Rule
 - GG. Regulatory Alternatives
 - HH. Comparative Analysis Between AIT and Alternatives
 - II. Other Comments on the Regulatory Impact Analysis
 - JJ. Initial Regulatory Flexibility Analyses
 - KK. Other Regulatory Analyses
 - LL. Comments on the Risk Analysis
 - MM. Other Comments on the NPRM
- III. Rulemaking Analyses and Notices
 - A. International Compatibility
 - B. Economic Impact Analyses
 - 1. Regulatory Impact Analysis Summary
 - 2. Executive Orders 12866 and 13563 Assessments
 - 3. Regulatory Flexibility Act Assessment
 - 4. International Trade Impact Assessment
 - 5. Unfunded Mandates Reform Act Assessment
 - C. Paperwork Reduction Act
 - D. Executive Order 13132, Federalism
 - E. Environmental Analysis
 - F. Energy Impact Analysis

I. Background**A. Summary of the Final Rule**

Congress has charged the Transportation Security Administration (TSA), a component of the U.S.

Department of Homeland Security (DHS), with responsibility for civil aviation security, 49 U.S.C. 114(d), including combatting the threat posed by al Qaeda and other terrorists. The Administrator of TSA must “assess current and potential threats to the domestic air transportation system” and take “necessary actions to improve domestic air transportation security,” including by providing for “the screening of all passengers and property” before boarding an aircraft to ensure that no passenger is “carrying unlawfully a dangerous weapon, explosive, or other destructive substance.” See 49 U.S.C. 44904(a) and (e); 44901(a); 44902(a)(1).

By Federal regulation, “[n]o individual may enter a sterile area or board an aircraft without submitting to the screening and inspection of his or her person and accessible property in accordance with the procedures being applied to control access to that area or aircraft. . . .” 49 CFR 1540.107(a). The final rule amends this regulation to specify that the screening and inspection of a person may include the use of advanced imaging technology (AIT).

Congress has directed the Secretary of Homeland Security to “give a high priority to developing, testing, improving, and deploying, at airport screening checkpoints, equipment that detects nonmetallic, chemical, biological, and radiological weapons, and explosives.” 49 U.S.C. 44925(a).¹ In June 2008, the Senate Appropriations Committee encouraged TSA to expand the use of AIT.² TSA began deploying AIT in 2008 after laboratory and operational testing.

The AIT currently deployed by TSA is a millimeter wave imaging technology that can detect metallic and non-metallic objects on an individual’s body or concealed in his clothing without physical contact. The technology bounces electromagnetic waves off the body to detect anomalies. If an anomaly is detected, a pat-down of the area where the anomaly is located is usually performed to determine if a threat is present.

AIT addresses a critical weakness in aviation security regarding the inability of walk-through metal detectors

(WTMDs) to screen for non-metallic explosives and other non-metallic threat items. AIT provides detection capability for weapons, explosives, and other objects concealed under a person’s clothing that may not trigger a metal detector. TSA has determined that use of AIT is the most effective technology currently available to detect both metallic and non-metallic threat items concealed on passengers, such as the non-metallic explosive used by the so-called “Christmas Day bomber” in 2009 in his attempt to blow up an American passenger aircraft.

AIT is an essential component of TSA’s risk-based security approach. This approach relies on a comprehensive security system including state-of-the-art technologies (such as AIT), a highly-trained frontline workforce, intelligence analysis and information sharing, behavior detection, explosives detection canine teams, Federal Air Marshals (FAMS), and regulatory enforcement.

In 2012, Congress enacted the FAA Modernization and Reform Act of 2012, Public Law 112–95, which required TSA to ensure that all AIT used to screen passengers must be equipped with and employ automatic target recognition (ATR) software. 49 U.S.C. 44901(l). That software eliminates passenger-specific (*i.e.*, individual) images and instead indicates the location of potential threats on a generic outline. Since May 2013, all AIT units deployed by TSA have been equipped with ATR capability. The final rule adopts the statutory definitions of AIT and ATR, and requires that any AIT equipment used to screen passengers be equipped with and employs ATR software.

There are approximately 793 AIT machines deployed at nearly 157 airports nationwide. AIT screening is safe for all passengers and the technology meets all national health and safety standards. Passengers generally may decline AIT screening and opt instead for a pat-down.

B. Purpose of the Final Rule

The final rule is adopted to comply with a ruling of the United States Court of Appeals for the District of Columbia Circuit. In *Electronic Privacy Information Center (EPIC) v. U.S. Department of Homeland Security*, 653 F.3d 1 (D.C. Cir. 2011), the court directed TSA to conduct notice-and-comment rulemaking on the use of AIT to screen passengers. TSA published a notice of proposed rulemaking (NPRM) on March 26, 2013, to obtain public comment on its proposal to revise civil aviation security regulations to codify

that TSA may use AIT for passenger screening. 78 FR 18287. The final rule defines AIT, states that AIT may be used to screen passengers, and requires that AIT be equipped with and employ the use of ATR software.

C. Costs and Benefits

When estimating the cost of a rulemaking, agencies typically estimate future expected costs imposed by a regulation over a period of analysis. As the AIT unit life cycle is 10 years from deployment to disposal, the period of analysis for estimating the cost of the rule is 10 years. TSA has revised the NPRM Regulatory Impact Analysis (RIA) assumption of an 8-year life cycle for AIT units to 10 years based on a recent life cycle cost estimate (LCCE) report.³ AIT deployment began in 2008 and TSA, therefore, includes costs that have already been borne by TSA, the traveling public, the screening systems industry, and airports. Consequently, this RIA takes into account costs that have already occurred—in years 2008–2014—in addition to the projected costs in years 2015–2017. By reporting the costs that have already occurred and estimating future costs in this manner, TSA accounts for the full life cycle of AIT machines.

TSA estimates the total cost of the rule from 2008–2017 to be \$2,146.31 million (undiscounted). TSA incurs over 98 percent of all costs.

AIT generates benefits by reducing security risks because it is capable of detecting both metallic and non-metallic weapons and explosives.⁵ Terrorists continue to test our security measures in an attempt to find and exploit vulnerabilities. The threat to aviation security has evolved to include the use of non-metallic explosives. Since it began using AIT, TSA has been able to detect many kinds of non-metallic items, small items, and items concealed on parts of the body that would not have been detected using the WTMD. TSA also considered the added benefit of deterrence—the effect of would-be

³ TSA’s Office of Security Capabilities (OSC), “Life Cycle Cost Estimate for Passenger Screening Program,” March 10, 2014. This is a TSA acquisition sensitive report based on OSC technology assessments.

⁴ The 2015 cost estimates used historical data when available. Please see the RIA for the complete description of the 2015 cost estimates.

⁵ Metal detectors and AITs are both designed to detect metallic threats on passengers, but do so in different ways. Metal detectors rely on the inductance that is generated by the metal, while AIT relies on the metal’s reflectivity properties to indicate an anomaly. AIT detection capabilities exceed that of metal detectors because AIT can detect metallic and non-metallic weapons, non-metallic bulk explosives, and non-metallic liquid explosives.

¹ See also Presidential Memorandum Regarding 12/25/2009 Attempted Terrorist Attack” (Jan. 7, 2010), available at <http://www.whitehouse.gov/the-press-office/presidential-memorandum-regarding-12252009-attempted-terrorist-attack> (charging DHS with aggressively pursuing enhanced screening technology in order to prevent further such attempts while at the same time protecting passenger privacy).

² S. Rep. No. 110–396, at 60 (2008).

attackers becoming discouraged because of increased security measures—from the use of AIT. Morral and Jackson (2009) stated, “Deterrence is also a major factor in the cost-effectiveness of many security programs. For instance, even if a radiation-detection system at ports never actually encounters weapon material, if it deters would-be attackers from trying to smuggle such material into the country, it could easily be cost-effective even if associated program costs are very high.”⁶ Given the demonstrated ability of AIT to detect concealed metallic and non-metallic objects, it is reasonable to assume that AIT acts as a deterrent to attacks involving the smuggling of a metallic or non-metallic weapon or explosive on board a commercial airplane. As an essential component in TSA’s comprehensive security system because it can detect both non-metallic and metallic threats concealed under a person’s clothing, AIT plays a vital role in decreasing the vulnerability of civil aviation to a terrorist attack.

To describe further the security benefits from AIT, TSA performed a break-even analysis to compare the potential direct costs of an averted terrorist attack to the net cost of AIT. Agencies use a break-even analysis when quantification of benefits is not possible. According to OMB Circular No. A-4, “Regulatory Analysis,” such an analysis answers the question, “How small could the value of the non-quantified benefits be (or how large would the value of the nonquantified costs need to be) before the rule would yield zero net benefits?”⁷ Based upon the results from the break-even analysis, TSA estimates that AIT will need to prevent an attack between once every 5.25 years to once every 23.5 years—depending on the size of the aircraft—for the direct cost of an averted attack to equal the annualized cost of AIT. The break-even analysis does not include the difficult to quantify indirect costs of an attack or the macroeconomic impacts that could occur due to a major attack. See Section III of this preamble for more

detailed results of the economic analyses.

D. Changes From the NPRM

In the NPRM, TSA proposed to amend 49 CFR 1540.107 by adding a new paragraph to specify that the screening and inspection of an individual prior to entering a sterile area of an airport or boarding an aircraft may include the use of AIT. TSA defined AIT as “screening technology used to detect concealed anomalies without requiring physical contact with the individual being screened.” TSA received many comments stating that the definition was too broad. Commenters also expressed confusion and uncertainty regarding the use of the word “anomalies.” Some commenters suggested privacy safeguards be included in the final rule.

In response to those comments, TSA changed the definition in the final rule. TSA is adopting the definition of AIT created by Congress in the FAA Modernization and Reform Act of 2012.⁸ That legislation, codified at 49 U.S.C. 44901(l), defines AIT as “a device used in the screening of passengers that creates a visual image of an individual showing the surface of the skin and revealing other objects on the body; and may include devices using backscatter x-rays or millimeter waves and devices referred to as ‘whole-body imaging technology’ or ‘body scanning machines’.” Further, in response to privacy concerns, TSA is adopting the statutory language that requires any AIT used for passenger screening to be equipped with and employ ATR software and comply with such other requirements TSA determines are necessary to address privacy considerations. Finally, consistent with the statute, TSA is defining ATR as, “software installed on an advanced imaging technology device that produces a generic image of the individual being screened that is the same as the images produced for all other screened individuals.”

In response to public comments, TSA also revised the RIA published with the NPRM to include a break-even analysis and pertinent data that has become available since the publication of the NPRM, including an updated AIT deployment schedule. TSA’s major changes to the RIA from the NPRM are:

- Revising the airport listings to include 460 airports instead of 448. The updated airport list includes new, previous, and former airports that operated AIT units and are regulated under 49 CFR part 1542.

- Updating the AIT life cycle and period of analysis from 8 to 10 years based on a recent LCCE report from the TSA Office of Security Capabilities (OSC). Using the information from this report, TSA also revised its previous assumption about the share of Passenger Screening Program expenditures spent on AIT technology.

- Revising the number of AIT units to be deployed from 821 to 793 throughout the period of analysis (2008–2017) based on new data.

- Revising the total wait time for a passenger that opts-out of AIT screening from 80 to 150 seconds to include passenger time spent waiting for a same gender Transportation Security Officer (TSO) to perform the pat-down.

- Revising the calculation of utilities costs to incorporate new data on the hours of AIT operation from the TSA’s Performance Management Information System (PMIS) database.

- Refining the calculation of personnel costs by using information on specific labor hours dedicated to AIT operation in response to new data on hours of AIT operation.

- Revising the calculation of training costs to incorporate newly available historical data on the hours of participation for each training course required for AIT operation and new training and development costs.

- Including a break-even analysis to answer the question, “How small could the value of the non-quantified benefits be (or how large would the value of the non-quantified costs need to be) before the rule would yield zero net benefits?”

- Revising language within the RIA and final rule to state that passengers “may generally opt-out of AIT screening” to reflect current DHS policy.⁹

Table 1 presents a summary of the effects of these changes. In the table, NPRM and final rule costs have been annualized due to the different periods of analysis.

⁶ Andrew R. Morral, Brian A. Jackson, “Understanding the Role of Deterrence in Counterterrorism Security,” 2009, Rand Homeland Security Program, http://www.rand.org/content/dam/rand/pubs/occasional_papers/2009/RAND_OP281.pdf.

⁷ http://www.whitehouse.gov/omb/circulars_a004_a-4/.

⁸ Public Law 112–95 (126 Stat. 11, Feb. 14, 2012).

⁹ See Privacy Impact Assessment Update for TSA Advanced Imaging Technology (DHS/TSA/PIA–032(d)) December 18, 2015, <https://www.dhs.gov/sites/default/files/publications/privacy-tsa-pia-32-d-ait.pdf>.

TABLE 1—CHANGES IN AIT ESTIMATES FROM THE NPRM TO THE FINAL RULE

[Annualized at a 7% discount rate in 2014 dollars]

Variables	NPRM and FR comparison			Description of changes
	NPRM	Final rule	Difference	
Annualized Industry Costs (\$millions)				
Airport Utilities Cost	\$0.19	\$0.15	– \$0.04	This estimate decreased due to incorporation of newly available historical data on AIT hours of operation from the TSA's PMIS database. Total cost in constant dollars remained the same, but annualized cost decreased because of the different periods of analysis between NPRM and final rule.
Backscatter AIT Removal	0.21	0.18	– 0.03	
Annualized Passenger Costs (\$millions)				
Opportunity Costs (Delay Costs).	2.08	2.60	0.52	This estimate increased because the estimated duration of a pat-down increased from 80 to 150 seconds to include passenger wait time to be handed off to a same gender TSO.
Annualized TSA Costs (\$millions)				
Personnel	216.40	117.17	– 99.22	TSA refined this estimate to account for labor hours dedicated to AIT operation. TSA used AIT operational hours recorded in PMIS as a basis for this estimate. TSA revised the calculation of training costs to incorporate newly available historical data on the hours of participation for each training course required for AIT operation and new training and development costs. TSA revised its cost estimates in 2014–2017 to reflect the most recent LCCE document by OSC. TSA also revised some assumptions for cost estimates from 2008–2013 based on the recent LCCE. This change reflects the revised estimate on AIT operation time and an increase of airport enrollment in TSAs utilities reimbursement program. The total cost decreased from the NPRM, primarily from the reduction in personnel costs.
Training	5.81	27.68	21.87	
Equipment	70.62	56.53	– 14.08	
TSA Utilities Cost	0.25	0.26	0.01	
Total Costs	¹⁰ 295.56	204.57	– 90.99	
Benefits				
Break-Even Analysis	Prevent 1 attack per 5.25 to 23.52 years considering only the major direct costs of an averted attack.			Per public comment, TSA has included a break-even analysis in the RIA.

II. Public Comments on the NPRM and TSA Responses

A. Summary

TSA published the NPRM on March 26, 2013, and requested comments be submitted by June 24, 2013. Private citizens, industry associations, advocacy groups, and non-profit organizations submitted comments in docket TSA 2013–0004. The discussion below groups the submissions by the primary issues raised in the public comments.

¹⁰ There was a calculation error in the NPRM's presentation of annualized costs. TSA has resolved this error and presented the correct annualized amounts in Table 1. The error in annualized cost did not affect any other cost estimates in the NPRM, including the estimated total cost of the rule and the estimated itemized costs presented in the NPRM.

B. Support for AIT

Comments: A number of submissions included a statement of general support for the continued use of AIT without offering additional, substantive rationale. Commenters also expressed approval for AIT for a variety of reasons. Several individual commenters stated they have medical conditions (e.g., metallic implants, metallic artificial joints, and prostheses) which cause them to alarm the WTMD, and they prefer the ease and quickness of AIT to the pat-down procedure, which would be required to resolve an alarm of the WTMD. Several other commenters noted that the need to ensure the safety of airline passengers and other American targets against terrorist threats outweighs possible privacy concerns associated with AIT. In supporting AIT use, many commenters referenced the

terrorist attacks on September 11, 2001. Individual commenters also stated they did not have any concerns related to the use of AIT. In response to other public comments opposed to AIT, several individual commenters questioned the significance of the alleged impact of AIT on privacy or safety. Several individual commenters also expressed a preference for AIT over a pat-down.

TSA Response: TSA agrees with these commenters that AIT provides the most effective and least intrusive means currently available to detect both metallic and non-metallic threats concealed under a person's clothing.

C. Opposition to AIT

Comments: Many submissions included statements of opposition to the continued use of AIT. Of these, individual commenters expressed concerns pertaining to efficacy, privacy,

health, cost, and civil liberties. TSA addresses each of these topics in subsequent comment responses in this preamble. Some individual commenters also expressed criticism of TSA and its staff. Some comments included statements requesting the elimination of AIT.

Other commenters made statements regarding the impact of AIT screening on their travel choices. Many of these commenters indicated they no longer travel by air because of the use of AIT. Some said they limit their airline travel as much as possible because of AIT screening. An individual commenter cited a news article that highlights increasing ridership of Amtrak over airline travel. Several other individual commenters noted that international travelers no longer want to visit the United States because of AIT screening. According to another individual commenter, the AIT scanners have created an “adversarial tension” between TSOs and travelers that is detrimental to security.

A few commenters discussed TSA’s statement in the NPRM that the public generally approves of the AIT scanners. For example, an individual commenter stated this claim was not supported by data regarding the public’s approval. Other commenters suggested that TSA should not assume the lack of complaints about AIT to be support for the use of AIT. For example, a privacy advocacy organization stated that TSA has not taken into consideration the number of passengers who choose AIT over a pat-down because it is faster and potentially less invasive of personal privacy, not because they support the use of AIT. Another individual commenter, however, acknowledged that National ABC and CBS news polls indicated that the majority of poll participants favored full body scanners at airports.

TSA Response: The information TSA receives from intelligence-gathering agencies confirms that civil aviation remains a favored target for extremists and terror organizations. AIT is an essential tool to address that threat by helping TSA to detect both metallic and nonmetallic explosives and other dangerous items concealed under clothing. AIT screening generally is optional and passengers are advised that they may choose to undergo a pat-down instead of AIT.

TSA takes the issues raised in the comments regarding the screening experience seriously and has instituted changes in its policies to address these concerns. New risk-based policies have transformed the agency from one that screens every passenger in the same

manner to one that employs a more effective, risk-based, intelligence-driven approach. Adopting a risk-based approach permits much-needed flexibility to adjust to changing travel patterns and shifting threats.

For example, beginning in 2011, after analyzing intelligence reports, TSA instituted new screening procedures for passengers under the age of 12 and those ages 75 and older to expedite screening and reduce the need for a pat-down to resolve alarms.¹¹ TSA also instituted TSA Pre✓™ (a known and trusted traveler program) based on the rationale that most passengers do not pose a risk to aviation security.¹² This program increases passenger throughput at the security checkpoint and improves the screening experience of frequent, trusted travelers.¹³ In addition, TSA Pre✓™ reduces the amount of time TSOs devote to screening low-risk travelers, thereby increasing the resources available to deter or detect the next attack. TSA is working to expand the population of passengers eligible for the program, the number of participating air carriers, and the airports where it is available. In December 2013, TSA launched its TSA Pre✓™ application program that allows U.S. citizens and lawful permanent residents to apply for TSA Pre✓™. As of February 2015, TSA Pre✓™ is available at 120 airports and eleven airlines participate in the program. Millions of passengers have undergone expedited screening through the program. Finally, TSA has instituted a new protocol at certain airports that allow passengers who are not registered in TSA Pre✓™ to undergo a real-time threat assessment at the airport so that they may be randomly selected for expedited screening. TSA will always incorporate random and unpredictable security measures throughout the airport, and no individual is guaranteed expedited screening. TSA encourages all potential passengers to learn about the

¹¹ These individuals currently can receive some form of expedited screening, are permitted to leave their shoes, light jackets, and headwear on for screening, and are screened primarily by the Walk-Through Metal Detector (WTMD). See <https://www.tsa.gov/travel/special-procedures>, <https://www.tsa.gov/travel/special-procedures/traveling-children>.

¹² <https://www.tsa.gov/tsa-precheck>.

¹³ <https://www.tsa.gov/tsa-precheck>. See also *Ruskai v. Pistole*, 775 F.3d 61, 64 (1st Cir. 2014) (“Additionally, TSA has opted to impose more limited screening burdens on passengers whom it confirms are part of TSA’s PreCheck program. As described in the briefing, PreCheck offers passenger members ‘expedited screening in designated lanes if they have been cleared for such screening based on certain background checks conducted prior to their arrival at the airport,’ and a more limited pat-down in the event that the passenger alarms a WTMD.”).

TSA Pre✓™ program by going to its Web site at www.tsa.gov.

As explained in the NPRM, in order to address privacy concerns and meet the statutory requirement to install and employ ATR software on all AIT units, TSA removed all backscatter AIT machines from screening checkpoints, and only millimeter wave AIT machines equipped with ATR are used to screen passengers. The ATR displays a generic outline on which boxes appear where an anomaly is detected. The outline is displayed on the AIT machine so that the passenger and the TSO are able to see the boxes. No specific image of an individual is created.

TSA disagrees with statements that use of AIT has had a material impact on U.S. air travel and the comments did not contain data in support. TSA was unable to find empirical evidence that air travel is reduced due to AIT. TSA notes that based on PMIS data collected from 2009, the first full year of data collection, through 2013, the last full year of data available at the time TSA began drafting this final rule, approximately one percent of passengers have selected a pat-down over AIT screening.¹⁴ TSA agrees with a commenter that independent polling on AIT acceptance shows strong public support for and understanding of the need for AIT.¹⁵

D. TSA Authority To Use AIT

Comments: Many individual commenters stated that TSA has overstepped its authority by deploying AIT and that the agency itself should be eliminated or that AIT should be eliminated as a screening technology. Additionally, many individual commenters stated that responsibility for airport security and the costs should be returned to either the owners of airports or the airlines.

A non-profit organization referenced 49 U.S.C. 44903(b)(2)(A) and 49 U.S.C. 44903(b)(2)(B) to support its statement that the proposed rule is inconsistent with statutory requirements to protect passengers and the public interest in promoting air transportation. The organization stated that TSA is not authorized “to sexually assault passengers” under current statutes or regulations. An individual commenter stated that TSA, as a Federal agency, has no jurisdiction over public airports, which the commenter stated are mostly on state land. Another individual commenter alleged that the

¹⁴ PMIS is a database used to track checkpoint operations. The database contains information on AIT use.

¹⁵ 78 FR 18296 at footnote 62.

Administrator of TSA acted illegally implementing AIT and stated he should be removed from office and charged accordingly.

TSA Response: TSA has the statutory authority to deploy AIT. The Administrator of TSA has overall responsibility for civil aviation security, and Congress has conferred on the Administrator authority to carry out that responsibility.¹⁶ Federal law requires that the Administrator “assess threats to transportation,” and “develop policies, strategies, and plans for dealing with threats to transportation security.”¹⁷

Prior to the terrorist attacks of September 11, 2001, and the enactment of the Aviation and Transportation Security Act (ATSA),¹⁸ air carriers were required to conduct the screening of passengers and property and did so in accordance with regulations issued by the Federal Aviation Administration (FAA) and security programs approved by the FAA.¹⁹ The security programs were sensitive security information (SSI) and were not shared with the public.²⁰ The ATSA transferred that responsibility to TSA, as codified at 49 U.S.C. 44901(a), and required the TSA Administrator to provide for the screening of all passengers and property that will be carried aboard a passenger aircraft. Federal law also requires the TSA Administrator to prescribe regulations to require air carriers to refuse to transport a passenger or the property of a passenger who does not consent to a search, and to protect passengers and property on an aircraft against an act of criminal violence or aircraft piracy.²¹ As commenters noted, when prescribing certain regulations, the Administrator is required to consider whether the regulation is consistent with protecting passengers and the public interest in promoting air transportation.²² Air transportation security is essential to ensure the freedom of movement for people and commerce. As the U.S. Court of Appeals for the First Circuit wrote in *Ruskai*, “[p]lanes blown out of the sky in Russia and attempted bombings on U.S. airliners in recent years have warned TSA that its screening procedures must be capable of detecting both metallic

and nonmetallic threats.”²³ TSA has determined that AIT is the best method currently available to screen passengers for both metallic and nonmetallic threats concealed under clothing.

As explained in the NPRM, Congress has directed that TSA prioritize the development and deployment of new technologies to detect all types of terrorist weapons at airport screening checkpoints, including the submission of a strategic plan to promote the optimal utilization and deployment of a range of detection technologies, including, “backscatter x-ray scanners.”²⁴ TSA has complied with this statute and with the subsequent statutory requirement that all AIT units used for passenger screening be equipped with ATR software, which eliminates passenger-specific images and only produces a generic outline.²⁵ Since May 16, 2013, all AIT units deployed by TSA have been equipped with ATR software; AIT units that could not accommodate ATR software have been removed from the airports.

E. Congressional Directive To Deploy AIT

Comments: Some commenters addressed the 2004 congressional directive discussed in the NPRM regarding the development and deployment of new screening equipment. An individual commenter noted that this congressional direction specifically included the investment in and deployment of AIT. Other commenters, however, stated that TSA’s implementation of AIT is inconsistent with congressional direction. Specifically, a privacy advocacy group stated that TSA’s deployment of AIT is inconsistent with a qualifier in the congressional directive—that the agency develop equipment to detect threats that terrorists would likely try to smuggle aboard an air carrier aircraft.²⁶ The commenter stated that TSA has demonstrated an overly broad interpretation of the congressional authorization and that, although the agency repeatedly cites AIT’s abilities to identify weapons, the NPRM does not establish how such weapons are likely to be smuggled aboard planes by terrorists. The commenter further stated that TSA must analyze and evaluate AIT and alternatives regarding the ability to detect weapons and explosives likely to

be used by terrorists, and demonstrate that AIT best achieves that goal with concrete evidence. The commenter stated that the analysis on which TSA currently relies fails to do either satisfactorily.

One individual commenter stated that a congressional directive is insufficient to supplant TSA’s duty to make a reasoned decision regarding the use of AIT. An individual commenter expressed concern that TSA did not act in accordance with the congressional direction because the agency acted without either public input or independent testing, and pursued a technology the commenter stated was purchased as part of a “corrupt deal.” Another individual commenter stated that Congress authorized TSA to procure and deploy AIT only as a secondary screening tool at security checkpoints—not as a primary means of screening. Other individual commenters stated that even if Congress has authorized the proposed deployment of AIT, the proposed use of AIT is not necessarily legal or the appropriate course of action, and TSA was not performing the agency’s own due diligence in trying to restrain the executive and legislative branches subsequent to congressional direction.

TSA Response: TSA is in compliance with Federal law, as well as congressional directives to pursue the development of new, advanced detection technology.²⁷ AIT addresses a critical vulnerability in aviation security. While WTMD and hand-held metal detectors are unable to screen for nonmetallic items, AIT can detect non-metallic explosives and other non-metallic threats, such as plastic firearms and knives. Explosives Trace Detection Devices (ETD) screen for nonmetallic explosives, but the process is too slow to perform on the same number of passengers as are currently screened by AIT. Congress clearly recognized this issue when it directed TSA to “give a high priority to developing, testing, improving, and deploying, at airport screening checkpoints, equipment that detects nonmetallic, chemical, biological, and radiological weapons, and explosives, in all forms, on individuals and in their personal property.”²⁸ There is no requirement in the statute or in any of the congressional reports to limit the use of AIT to secondary screening.

AIT provides greater detection capability for weapons, explosives, and other threats concealed on a passenger’s body that may not trigger a metal

¹⁶ 49 U.S.C. 114(d).

¹⁷ 49 U.S.C. 114(f).

¹⁸ Public Law 107–71 (115 Stat. 597, Nov. 19, 2001).

¹⁹ 14 CFR part 108, 66 FR 37330 (July 17, 2001). The FAA Administrator prescribed regulations requiring air carriers to screen all passengers and property before boarding.

²⁰ See 14 CFR 191.7(a) (2001).

²¹ 49 U.S.C. 44902(a) and 44903(b).

²² 49 U.S.C. 44903(b)(1), (2), and (3).

²³ *Ruskai v. Pistole*, 775 F.3d, 61, 63 (1st Cir. 2014).

²⁴ 49 U.S.C. 44925(a) and (b). “Detection Equipment at Airport Screening Checkpoints,” Report to Congress, Aug. 9, 2005. See also 78 FR 18292.

²⁵ 49 U.S.C. 44901(l).

²⁶ 49 U.S.C. 44925(a).

²⁷ See 49 U.S.C. 44925(a) and 44901(l).

²⁸ 49 U.S.C. 44925(a).

detector. Concealed threat items, including nonmetallic explosives, pose a substantial threat to aviation security. As the former TSA Administrator explained in an August 2013 speech to the Airports Council International/North America, “With respect to the evolving security challenges we all face today, one of the principal concerns we have is the continued migration to more nonmetallic threats such as liquid and plastic explosives.”²⁹ As explained in the NPRM, on December 25, 2009, a bombing plot by Al Qaeda in the Arabian Peninsula (AQAP) culminated in Umar Farouk Abdulmutallab’s attempt to blow up an American aircraft over the United States using a non-metallic explosive device hidden in his underwear. 78 FR 18291. More recently, in the spring of 2012, AQAP developed another concealed, nonmetallic explosive that had a new level of redundancy in the event the primary system failed. Fortunately, this plot was thwarted.³⁰ Additionally, open source information shows that terrorists currently plan to conduct attacks against the United States. Terrorists test the limits of TSA’s ability to detect nonmetallic explosives concealed under clothing; the destruction of passenger aircraft remains a terrorist priority.

F. Compliance With the Administrative Procedure Act

Comments: Some commenters addressed concerns related to the Administrative Procedure Act (APA). Generally, commenters stated that TSA has not complied with the APA’s procedural requirements. Non-profit organizations, a privacy advocacy group, and individual commenters stated that TSA did not comply with APA requirements prior to initial deployment of AIT. A privacy advocacy group stated that the agency received two petitions signed by numerous civil liberties organizations to institute a rulemaking proceeding, yet failed to initiate such a proceeding. A few individual commenters stated that if TSA had initially complied with rulemaking procedures, the public likely would have rejected the proposed action, and TSA would not have been able to deploy the technology. A privacy advocacy group and an individual

commenter raised further concerns regarding the money spent on the deployment of AIT despite the lack of opportunity for public comment.

Commenters stated that the proposed rule and justification provided in the NPRM would not meet the arbitrary and capricious standard applied to agency actions under the APA. A privacy advocacy group stated that factors regarding effectiveness, alternatives, and health risks were not considered and the term “anomaly” was not adequately explained.

Commenters also stated that the proposed regulatory language effectively failed to provide the public with adequate notice and denied the public the opportunity to provide meaningful comment because the rule is too broad and vague, and descriptive information on the program was omitted.

An individual commenter wrote that noncompliance with APA requirements indicated TSA acts as it chooses without accountability. Another individual commenter requested TSA to commit to complying with APA requirements in the future. A non-profit organization requested that TSA hold public hearings in the future before imposing new procedures and policies, but specified that the agency should retain the authority to declare emergency regulations and procedures without public hearings or a comment period. Further, an individual commenter suggested that TSA withdraw the proposed rule and issue an advance notice of proposed rulemaking to allow TSA to gather missing information in order to receive comments that are more meaningful. An advocacy group and an individual commenter stated that TSA only issued a NPRM because it was court-ordered. Other commenters wrote that TSA had the option to request public input prior to implementing and deploying AIT scanners.

TSA Response: As discussed above, TSA deployed AIT consistent with its statutory authority and as directed by Congress. TSA issued the NPRM consistent with the opinion of the U.S. Court of Appeals for the DC Circuit in *EPIC v. DHS*, 653 F.3d 1 (D.C. Cir. 2011). In that case, TSA contended it had properly processed letters it received from EPIC and other groups regarding the initiation of a rulemaking proceeding. TSA also described how the deployment of AIT was consistent with statutory exceptions to the notice-and-comment requirements of the APA. The court did not agree. “None of the exceptions urged by the TSA justifies its failure to give notice of and receive

comments upon such a rule.”³¹ The court explained that,

[d]espite the precautions taken by the TSA, it is clear that by producing an image of the unclothed passenger, an AIT scanner intrudes upon his or her personal privacy in a way a magnetometer does not. Therefore, regardless whether this is a ‘new substantive burden,’ . . . the change substantively affects the public to a degree sufficient to implicate the policy interests animating notice-and-comment rulemaking.³²

A subsequent decision by the same court, however, indicates that TSA’s decision not to engage in rulemaking prior to deploying AIT was not unreasonable. Following the court’s APA ruling, EPIC petitioned the court to recover attorney’s fees under the Equal Access to Justice Act (EAJA). 28 U.S.C. 2412(d). The EAJA allows attorney’s fees to be recovered unless the position of the government “was substantially justified or . . . special circumstances make an award unjust.”³³ In denying EPIC’s request to recover attorney’s fees, the court stated, “[t]he TSA’s position regarding the only issue on which EPIC prevailed—whether the agency improperly bypassed notice and comment in adopting the new screening technology—was substantially justified.”³⁴

Federal regulation stipulates that no individual may enter the sterile area of an airport or board an aircraft without submitting to the screening and inspection of his or her person and accessible property “in accordance with the procedures being applied to control access to that area or aircraft. . . .” 49 CFR 1540.107(a). This requirement was originally promulgated by the FAA through notice and comment rulemaking and then transferred to TSA by ATSA.³⁵

Although TSA acknowledges that it did not engage in notice and comment rulemaking related to the deployment of AIT specifically prior to its use, TSA does not agree with statements by commenters that there was no public notice of TSA’s use of AIT. Prior to the deployment of AIT, TSA conducted years of testing on the safety, effectiveness, and efficiency of the

³¹ *EPIC*, 653 F.3d at 11.

³² *Id.* at 6.

³³ 28 U.S.C. 2412(d)(1)(A).

³⁴ *EPIC v. DHS*, No. 10–1157 (Order filed Feb. 15, 2012).

³⁵ See 62 FR 41730, 63 FR 19691, and 66 FR 37330, 37360. The ATSA transferred that authority from FAA to TSA in 2001. On February 22, 2002, the TSA and FAA published a final rule titled “Civil Aviation Security Rules,” 67 FR 8340, transferring the regulations at 14 CFR parts 107, 108, 109 and 191 to 49 CFR parts 1540, 1542, 1544, 1548, and 1520, and §§ 129.25 and 129.26 to part 1546.

²⁹ John S. Pistole, TSA Administrator, address at the Airports Council International–North America (Aug. 14, 2013). Text available at <https://www.tsa.gov/news/speeches/airports-council-international-%E2%80%93-north-america-tsa-administrator-john-s-pistole-0>.

³⁰ *Id.* Note that these examples occurred on flights originating outside of the United States. Therefore, TSA’s AIT would not have been in place to detect the devices.

technology.³⁶ Contrary to the assertion of a commenter regarding the purchase of AIT equipment, the AIT equipment was obtained in accordance with all government procurement requirements, which includes the public solicitation of bids.³⁷ TSA also considered alternatives to AIT and these are discussed in the NPRM and the RIA. In 2007, TSA initiated the first pilot test of AIT in the secondary screening position. In January 2008, TSA published a Privacy Impact Assessment (PIA), which encompassed AIT screening of all passengers, both as a primary and secondary form of passenger screening.³⁸ The PIA provided notice to the public regarding TSA's use of the technology. It stated that TSA published extensive information on the technology on its Web site beginning in February 2007 and conducted outreach with national press and with privacy advocacy groups to explain the evaluation of the technology. The PIA explained that informational brochures were made available to the public at each pilot site showing the image that the technology created. The cover page of each PIA includes a point of contact for the public to reach out to with questions or concerns. In 2009, TSA began to test AIT as the primary screening equipment. In 2010, TSA submitted a Report to Congress on privacy protections and deployment of AIT.³⁹ TSA also published information on its Web site to inform passengers of AIT procedures at the checkpoint at www.tsa.gov. The public may provide comments or concerns regarding AIT by contacting the TSA Contact Center.⁴⁰

As directed by the court, TSA issued the NPRM and invited public comment on its proposed regulation regarding the use of AIT for primary screening of passengers. The NPRM invited public comment on a variety of issues related

to the use of AIT, including the threat to aviation security, types of AIT equipment, privacy safeguards, safety, AIT procedures and items discovered using AIT. TSA received thousands of comments on these issues. In response to comments and to avoid confusion, TSA has altered the regulatory text in the final rule. TSA has determined not to define AIT using the term "anomaly"; instead, TSA has adopted the statutory definition of AIT, *i.e.*, a device used in the screening of passengers that creates a visual image of an individual showing the surface of the skin and revealing other objects on the body. In addition, TSA has clarified the final rule by adopting the statutory provision to deploy AIT equipped with ATR software. Thus, AIT equipment must produce a generic image of the individual being screened that is the same as the images produced for all other screened individuals. These changes are in response to the concerns of commenters regarding the breadth of the regulatory text, and significantly mitigate any privacy concerns associated with the use of AIT as a primary screening method. Accordingly, and consistent with TSA's obligation to complete this rulemaking and TSA's discretion to prioritize its rulemaking resources, TSA does not intend to issue a supplemental NPRM or hold public hearings on this matter. TSA addresses issues regarding effectiveness and safety in subsequent responses.

G. Adherence to the Court Decision in *EPIC v. DHS*

Comments: Commenters also discussed the court's decision in *EPIC v. DHS*. Several individual commenters specifically supported EPIC's position that AIT scanners are invasive of individual privacy. Another individual commenter opposed the court's decision to allow TSA to continue use of AIT. A privacy advocacy group wrote that the NPRM incorrectly stated the holding of the case. A privacy advocacy group and many individual commenters pointed out the length of time that elapsed between the court decision and the issuance of the NPRM. A privacy advocacy group stated that it filed three mandamus petitions during the elapsed 2-year period. An advocacy group stated that the constitutional issue raised by EPIC was not ripe for decision because the court did not have a rulemaking record before it and speculated that the court might invalidate its holding regarding the Fourth Amendment in a future judicial review of this rulemaking.

TSA Response: TSA is in compliance with the court's directive to engage in

notice-and-comment rulemaking on the use of AIT to screen passengers. TSA notes that all of EPIC's other constitutional and statutory challenges to the use of AIT, including its Fourth Amendment claims, were rejected by the court. The court also rejected EPIC's petition for rehearing (including the Fourth Amendment ruling), as well as three subsequent petitions that EPIC filed demanding immediate issuance of the NPRM. TSA notes that the court issued its decision before TSA instituted ATR software on all of the millimeter wave AIT units and removed all of the backscatter units from service. The ATR software does not produce an individual image of a passenger that must be reviewed by a TSO, but instead reveals a generic outline that is visible to the passenger as well as the TSO. In a recent case decided after these changes in AIT equipment were implemented, the U.S. Court of Appeals for the First Circuit held that a constitutional challenge to AIT body scanners that depict revealing images of bodies and pat-downs procedures for passengers who opted out of screening using AIT became moot following the installation of ATR software on all millimeter wave units and the removal of backscatter machines.⁴¹

H. Fourth Amendment Issues

Comments: Commenters also addressed concerns related to the Fourth Amendment. The vast majority of these commenters stated that use of AIT constitutes a violation of Fourth Amendment rights. Individual commenters stated that AIT fails to meet the standard of a constitutionally permissible search. Specifically, some individual commenters stated that TSA could not conduct such searches without a warrant. Individual commenters also stated that neither the purchase of an airline ticket nor a desire to travel is sufficient to give TSA "probable cause" to conduct a search.

Others stated that AIT is impermissible under Federal case law. Several individual commenters cited the holding in *U.S. v. Davis*, in which the U.S. Court of Appeals for the Ninth Circuit held that administrative searches must be "no more extensive nor intensive than necessary, in the light of current technology, to detect the presence of weapons or explosives, that it is confined in good faith to that purpose, and that potential passengers may avoid the search by electing not to

³⁶ See, e.g., "Detection Equipment at Airport Screening Checkpoints," Report to Congress, Aug. 9, 2005. The report describes TSA's ongoing research and development program to develop technologies to increase its ability to detect explosives on passengers, including body imaging systems, *i.e.*, backscatter x-ray.

³⁷ See The TSA is seeking sources for Imaging Technology systems, Solicitation No. HSTS04-08-R-CT2056, https://www.fbo.gov/index?s=opportunity&mode=form&id=be7cd5b087bd3d28ce6bee81f7644141&tab=core&_cview=1.

³⁸ "Privacy Impact Assessment for TSA Whole Body Imaging," Jan. 2, 2008. Updates to the initial AIT PIA were conducted on Oct. 17, 2008, Jul. 23, 2009, and Jan. 25, 2011. See <http://www.dhs.gov/publication/dhstapia-032-advanced-imaging-technology>. All TSA PIA reports are available at <http://www.dhs.gov/privacy-documents-transportation-security-administration-tsa>.

³⁹ "Advanced Imaging Technologies: Passenger Privacy Protections," Fiscal Year 2010 Report to Congress, Feb. 25, 2010.

⁴⁰ <https://www.tsa.gov/contact>.

⁴¹ *Redfern v. Napolitano*, 727 F.3d 77, 83–85 (1st Cir. 2013).

fly.”⁴² Several individual commenters stated that the AIT screening process fails to meet this standard because elements of the scan and the opt-out alternative are too intrusive, and the scope of the scan is not tailored narrowly enough to exclusively identify weapons, explosives, and incendiaries (e.g., AIT is able to identify items such as adult diapers and women’s sanitary products, which commenters stated are outside the scope of threats TSA is trying to identify). Individual commenters recommended alternative search methods that they thought were less invasive and better suited to meet TSA’s need, such as x-raying suitcases, using WTMD, and only using AIT as a secondary means of screening.

Other court cases cited in the comments to support claims that AIT violates the Fourth Amendment include: *U.S. v. Pulido-Baquerizo*, 800 F.2d 899 (9th Cir. 1986), *U.S. v. Skipwith* 482 F.2d 1272 (5th Cir. 1973), *U.S. v. Hartwell*, 436 F.3d 174 (3d Cir. 2006), *Camara v. Municipal Court*, 387 U.S. 523 (1967), *Missouri v. McNeely*, 133 S.Ct. 1552 (2013), *Katz v. U.S.*, 389 U.S. 347 (1967). An individual commenter also cited a court decision pertaining to virtual strip searches, *Reynolds v. City of Anchorage*, 379 F.3d 358 (6th Cir. 2004) to support opposition to AIT.

An individual commenter observed that, even though AIT use was not found to be in violation of the Fourth Amendment in *EPIC v. DHS*, the subsequent issuance of an NPRM, which does not specify the degree to which AIT will be used to promote the government’s interest, may result in TSA’s failure to meet the balancing test applied to Fourth Amendment rights cases.

TSA Response: The court in *EPIC* held that the use of AIT as a primary screening method at an airport security checkpoint does not violate the Fourth Amendment.⁴³ This decision is consistent with decisions by the U.S. Supreme Court and the Federal circuits that have upheld airport security screening as a valid administrative search that does not require a warrant, probable cause, reasonable suspicion, or the consent of the passenger.⁴⁴ More

than 30 years ago, the U.S. Court of Appeals for the Third Circuit recognized that the government “unquestionably has the most compelling reasons,” including “the safety of hundreds of lives and millions of dollars’ worth of private property for subjecting airline passengers to a search for weapons and explosives.” *Singleton v. Comm’r of Internal Revenue*, 606 F.2d 50, 52 (3d Cir. 1979). “[T]he events of September 11, 2001, only emphasize the heightened need to conduct searches at this nation’s international airports.” *U.S. v. Yang*, 286 F.3d 940, 944 n.1 (7th Cir. 2002). In a recent opinion issued by the U.S. Court of Appeals for the Eleventh Circuit, the Court concluded that AIT “is a reasonable administrative search under the Fourth Amendment.”⁴⁵

Like other exceptions created by courts for searches that do not require a warrant, the administrative search within the airport context reflects the careful balancing of the public’s privacy interests against the compelling goal of protecting the traveling public. As explained by the D.C. Circuit in *EPIC*, because the primary goal of airport screening is “not to determine whether any passenger has committed a crime but rather to protect the public from a terrorist attack,” airport screening is permissible under the Fourth Amendment without individualized suspicion so long as the government’s interest in conducting screening outweighs the degree of intrusion on an individual’s privacy.⁴⁶ The court made clear that this standard does not require the government to use the least intrusive search method possible.⁴⁷ In fact, the U.S. Supreme Court has held that the scope of the administrative search must be “reasonably related to [its] objectives” and “not excessively intrusive.”⁴⁸ In *EPIC*, the court found that the—

balance clearly favors the Government here. The need to search airline passengers ‘to ensure public safety can be particularly acute,’ and, crucially, an AIT scanner, unlike a magnetometer, is capable of detecting, and

commercial airlines . . . without any basis for suspecting any particular passenger of an untoward motive.”), *U.S. v. Aukai*, 497 F.3d 955, 960 (9th Cir. 2007) (en banc) (“The constitutionality of an airport screening search, however, does not depend on consent.”).

⁴⁵ *Corbett v. TSA*, 767 F.3d 1171, 1180 (11th Cir. 2014) (“The scanners at airport checkpoints are a reasonable administrative search because the governmental interest in preventing terrorism outweighs the degree of intrusion on . . . privacy and the scanners advance that public interest.”).

⁴⁶ *EPIC*, 653 F.3d at 10.

⁴⁷ *Id.* at 10–11.

⁴⁸ *City of Ontario v. Quon*, 560 U.S. 746, 761 (2010) (internal quotation marks omitted).

therefore of deterring, attempts to carry aboard airplanes explosives in liquid or powder form. On the other side of the balance, we must acknowledge the steps TSA has already taken to protect passenger privacy, in particular distorting the image created using AIT and deleting it as soon as the passenger has been cleared.⁴⁹ [Citations omitted]

With the addition of ATR software and the elimination of any individual image, the balance tips even more in favor of the government. Courts have also held that, “absent a search, there is no effective means of detecting which airline passengers are reasonably likely to hijack an airplane.”⁵⁰

Commenters’ claims and citations to support the position that the least intrusive search method must be adopted are contrary to U.S. Supreme Court precedent in *Quon*, as well as the *EPIC* decision. In fact, the court in *EPIC* specifically rejected the argument that *U.S. v. Hartwell*, cited in many of the comments, stands for the proposition that AIT scanners must be minimally intrusive to be consistent with the Fourth Amendment.⁵¹ Moreover, especially following the universal deployment of ATR software, TSA believes that the use of AIT as a primary screening method is not intrusive. The scan and the results require just a few seconds. Passengers are not subjected to any physical intrusion. The only potential for invasiveness occurs when AIT alarms, thereby requiring additional screening to verify whether a threat item is present.⁵² Passengers are instructed through TSA’s Web site and cautioned before they enter the AIT unit to remove all items from their pockets to prevent an alarm.

TSA is not required to use any of the alternatives to AIT mentioned in the comments to achieve the legal requirements of a valid search. For example, all baggage, whether checked or carry-on, is already screened as required under 49 U.S.C. 44901. Limiting an airport search to baggage, however, would not address the threat that a person could conceal an explosive on his or her person. The government has latitude under the Fourth Amendment to choose among

⁴⁹ *EPIC*, 653 F.3d at 10.

⁵⁰ See *Singleton v. Comm’r of Internal Revenue*, 606 F.2d 50, 52 (3d Cir. 1979). See also *U.S. v. Marquez*, 410 F.3d 612, 616 (9th Cir. 2005) (“Little can be done to balk the malefactor after weapons or explosives are successfully smuggled aboard, and as yet there is no foolproof method of confining the search to the few who are potential hijackers.”) (quoting *Davis*, 482 F.2 at 910)).

⁵¹ *EPIC*, 653 F.3d at 10–11.

⁵² In other limited circumstances, based on the particular item of clothing, TSA may require additional screening even if the AIT does not alarm.

reasonable alternatives for conducting an administrative search.⁵³ AIT is the only technology that will find both metallic and non-metallic items, and will find both explosives and non-explosives items. The WTMD only finds metallic items, thus does not find such threats as explosive devices made without metal, or other non-metallic items. The ETD will find only explosives, not metallic items (such as firearms) or non-metallic items that are not explosives (such as ceramic knives); the same is true for explosives detection canines. Pat-down screening is useful for finding both metallic and non-metallic items, and will find both explosives and non-explosives items, however, that method is slower than AIT and many persons consider pat downs to be more intrusive than AIT.

The other cases cited in the comments, particularly those relating to whether consent is required for airport screening, are inapplicable. Both *U.S. v. Davis*, 482 F.2d 893 (9th Cir. 1973) and *U.S. v. Pulido-Baquerizo*, 800 F.2d 899 (9th Cir. 1986) regarding whether a passenger must consent to a search, have been superseded by the decision of the U.S. Court of Appeals for the Ninth Circuit in *U.S. v. Aukai*.⁵⁴ In *Aukai*, the court confirmed that airport screening searches are constitutionally reasonable administrative searches and clarified that the reasonableness of such searches does not depend, in whole or in part, upon the consent of the passenger being searched.⁵⁵ *U.S. v. Skipwith*, 482 F.2d 1272 (5th Cir. 1973), deals with a law enforcement search based on suspicion, which is not required for the administrative search performed by TSA. Neither *Camara v. Municipal Court*, 387 U.S. 523 (1967), *Missouri v. McNeely*, 133 S. Ct. 1552 (2012), nor *Katz v. U.S.*, 389 U.S. 347 (1967) involves the administrative search conducted by TSA at airport security checkpoints, which courts have consistently found is justified by the compelling government interest in protecting the traveling public.⁵⁶

⁵³ *Quon*, 560 U.S. at 764 (“Even assuming there were ways that [the government] could have performed the search that would have been less intrusive, it does not follow that the search conducted was unreasonable.”).

⁵⁴ *U.S. v. Aukai*, 497 F.3d 955 (9th Cir. 2007) (en banc).

⁵⁵ *Aukai*, 497 F.3d at 957.

⁵⁶ See generally *Marquez*, 410 F.3d 612, 618 (“It is hard to overestimate the need to search air travelers for weapons and explosives”) and *Singleton*, 606 F.2d 50, 52 (“the government unquestionably has the most compelling reasons . . . for subjecting airline passengers to a search for weapons or explosives that could be used to hijack an airplane.”). The facts in *Camara* involved the attempted search of a home without a warrant. The Supreme Court found that the government was not

Finally, the reference to strip search cases by a commenter is not applicable to AIT given the privacy restrictions TSA used when it first deployed AIT and even more so now that all AIT units are equipped with ATR software and do not display an individual image. In addition, the AIT units do not have the ability to store, print, or transmit any images. As noted previously, a TSO does not usually touch a passenger's body unless the AIT alarms. With ATR, there is no individual image of a traveler; the generic outlines produced are so innocuous that they are displayed publicly at the airport.

I. Other Legal Issues

Comments: Commenters raised other legal issues in opposing AIT. Several individual commenters, a non-profit organization, and several advocacy groups stated that AIT scanning and/or opt-out process violates rights guaranteed by the First, Second, Fifth, Sixth, Eighth, Ninth, Tenth, and Fourteenth Amendments, respectively. Commenters did not generally provide further substantive legal arguments in support of these constitutional claims. An advocacy group, however, cited a Supreme Court case, *Aptheker v. Sec'y of State*, 378 U.S. 500, 505 (1964), which held that if a law “too broadly and indiscriminately restricts the right to travel” it “thereby abridges the liberty guaranteed by the Fifth Amendment.” The commenter further stated that the court considered relevant “that Congress has within its power ‘less drastic’ means of achieving the congressional objective of safeguarding our national security.” An individual commenter cited *U.S. v. Guest*, 383 U.S. 745 (1966) and *Shapiro v. Thompson*, 394 U.S. 618 (1969) in opposing the use of AIT. Another advocacy group cited 49 U.S.C. 40101, 40103, and the International Covenant on Civil and Political Rights, a treaty that the U.S. has ratified, as further reinforcing the right to travel. The commenter remarked that the NPRM does not recognize that travel by air and, specifically, by common carrier, is a right and that TSA must evaluate its proposed actions within that context. Similarly, an individual commenter stated that TSA's use of AIT involves limitations on constitutional rights and, therefore,

able to articulate a special need or legitimate public interest to justify dispensing with the requirement to obtain a warrant. In *McNeely*, a blood test of a person suspected of driving while intoxicated was obtained without a warrant. In *Katz*, the Supreme Court held that electronically listening to and recording an individual's conversation at a public telephone booth without a warrant violated the Fourth Amendment.

strict scrutiny should be the judicial review standard applied. Another individual commenter stated that implementation of AIT scanners assumes travelers' guilt, which is in violation of the principle of the presumption of innocence.

One individual commenter stated that it is outside of TSA's mission to identify and confiscate items that are not a threat (e.g., illegal drugs) and that such “mission creep” is an inappropriate use of Federal funds and distracts TSA staff from their actual mission. Other individual commenters stated that AIT and pat-downs violate laws prohibiting sexual molestation. A non-profit organization suggested that TSA review and modify its policies to ensure that they do not conflict with existing state law procedures protecting children from physical and sexual assault or with existing child protective services legislation.

TSA Response: As to the claims of violations of the Constitution, as explained in the response to the previous grouping of comments, in recognition of the importance of the safety concerns at issue, courts have regularly upheld airport screening procedures against constitutional challenges. Thus, it is well settled as a matter of law that an airport screening search conducted to protect the safety of air travelers is a legitimate exercise of government authority and does not impinge on any of the constitutional amendments listed in the comments. Passengers are on notice that their persons and their property are subject to search prior to entering the sterile area of the airport or boarding an aircraft. Federal law requires “the screening of all passengers and property” before boarding an aircraft to ensure no passenger is “carrying unlawfully a dangerous weapon, explosive, or other destructive substance.” 49 U.S.C. 44901(a) and 44902(a). Federal law also requires commercial air carriers to prevent anyone from boarding who does not submit to security screening. 49 U.S.C. 44902(a).

The use of AIT to conduct passenger screening does not implicate any constitutional rights in the manner described in the comments. Passengers are not restricted regarding their speech or right to assemble so long as they do not interfere with screening.⁵⁷

⁵⁷ Interference with screening is prohibited by 49 CFR 1540.109. TSA defines interference in part as that which “might distract or inhibit a screener from effectively performing his or her duties,” to include verbal abuse of screeners by passengers or air crew, but not good-faith questions from individuals seeking to understand the screening of

Continued

Passengers may transport unloaded firearms in checked baggage in a locked, hard-sided container, thus, there is no infringement of Second Amendment rights. 49 CFR 1540.111. In general, the Fifth, Sixth, and Eighth Amendments have to do with the rights of persons accused of a crime and have no relevance to airport security screening conducted by TSA. Federal law requires that screening be conducted on all passengers and property prior to boarding an aircraft, and rights reserved for citizens or the states, discussed in the Ninth and Tenth Amendments respectively, are not impacted by airport screening. Comments invoking the Fourteenth Amendment generally did so without specifying which clause of the Amendment is at issue or how it was implicated by AIT, or invoked it in connection with non-AIT aspects of TSA screening.

Federal courts have long held that airport screening searches do not violate a traveler's right to travel.⁵⁸ "Air passengers choose to fly, and screening procedures . . . have existed in every airport in the country since at least 1974."⁵⁹ The holding in *Aptheker*, cited by a commenter, pertained to whether Section 6 of the Subversive Activities Control Act of 1950, which restricted members of Communist organizations in obtaining or using a passport, was constitutional. It has no application to the use of AIT to conduct airport screening, which does not restrict a person's right to travel, the ability to obtain a passport, or the ability to obtain documentation necessary to enter a country legally. Further, the Ninth Circuit Court of Appeals has held that TSA's regulation requiring passengers to present identification prior to entering a sterile area or boarding an aircraft, 49 CFR 1540.107(b), does not violate any Constitutional rights.⁶⁰

As to the comment regarding the confiscation of items that are not a

their persons or property. See 67 FR 8340, 8344 (Feb. 22, 2002). Interference with screening might also include passenger activity that requires a screener to "turn away from his or her normal duties to deal with the disruptive individual," or might "discourage the screener from being as thorough as required." See *id.*; 49 CFR 1540.109; *Rendon v. TSA*, 424 F.3d 475 (6th Cir. 2005) (constitutional rights not infringed when penalty was imposed on traveler who became loud and belligerent after he set off metal detector alarm which required screener to shut down his line and call over his supervisor).

⁵⁸ *U.S. v. Davis*, 482 F.2d 893 (9th Cir. 1973).

⁵⁹ *Hartwell*, 436 F.3d at 174.

⁶⁰ *Gilmore v. Gonzales*, 435 F.3d 1125, 1136–1137 (9th Cir. 2006) ("We reject Gilmore's right to travel argument because the Constitution does not guarantee the right to travel by any particular form of transportation . . . Gilmore does not possess a fundamental right to travel by airplane even though it is the most convenient mode of travel for him.").

security threat such as illegal drugs, the purpose of TSA screening is to prevent weapons, explosives, and other items that could pose a security threat (prohibited items) from being carried into the sterile area of the airport or onboard an aircraft in order to ensure the freedom of movement for people and commerce. 49 CFR 1540.111. TSA's mission has not changed. TSOs do not search for other illegal items. When searching for prohibited items, however, it is not unusual for TSOs to uncover items that may be evidence of criminal activity. When that happens, the TSO turns such matters over to law enforcement officers to resolve, consistent with applicable criminal statutes. TSOs do not take possession of such items. In addition, once an anomaly is detected by AIT, or a metal object is detected by a WTMD, or either screening system misalarms, additional screening must take place to determine whether there is an item, and if so, if the item detected is a threat to aviation security. As the court in *Hartwell* noted, "Even assuming that the sole purpose of the checkpoint was to search only for weapons or explosives, the fruits of the search need not be suppressed so long as the search itself was permissible. . . . Since the object in *Hartwell*'s pocket could have been a small knife or bit of plastic explosives, the TSA agents were justified in examining it."⁶¹

TSA's pat-down procedures are designed to ensure that any touching of the body by a TSO is minimally intrusive while effectively screening for prohibited items. A TSO does not touch a passenger's body unless necessary to resolve an AIT alarm, or unless the passenger has opted for a pat-down, and the procedures are largely similar to those employed to resolve WTMD alarms. Touching of the body to perform this essential security function is fully within the scope of TSA's authority, and TSA's procedures are consistent with civil and criminal state laws. Sexual molestation or inappropriate touching of a passenger by an employee is strictly prohibited and TSA has procedures in place to investigate any allegations of such conduct thoroughly. TSA takes all allegations of misconduct seriously.

Passengers who believe they have experienced unprofessional conduct at a security checkpoint may request to speak to a supervisor at the checkpoint or write to the TSA Contact Center at TSA-ContactCenter@dhs.gov. Passengers who believe they have been

⁶¹ *Hartwell*, 436 F.3d at 181 n.13. See also *Marquez*, 410 F.3d at 617 ("The screening at issue here is not unreasonable simply because it revealed that Marquez was carrying cocaine rather than C-4 explosives.").

subject to discriminatory treatment at the checkpoint may file a complaint with TSA's Office of Civil Rights & Liberties, Ombudsman and Traveler Engagement (OCRL/OTE) at TSA-CRL@tsa.dhs.gov, or submit an online complaint at <https://www.tsa.gov/contact-center/form/complaints>.⁶² The Office of Inspection, in addition to OCRL/OTE and management, may investigate misconduct allegations. Travelers may also file discrimination complaints concerns with the DHS Office for Civil Rights and Civil Liberties (CRCL) via CRCL's Web site at <http://www.dhs.gov/complaints>. In addition, as discussed further below, TSA has amended its screening procedures to modify the pat-down used when necessary to screen children age 12 and under and adults age 75 and older and has reduced the instances where such passengers would be subject to a pat-down.

J. Evolving Threats to Security

Comments: Commenters also addressed the evolving threats to aviation security discussed by TSA in the NPRM. Some commenters stated that TSA's screening efforts are not linked to the decrease in aircraft-related terror attempts since September 11, 2001. For example, individual commenters and a non-profit organization stated that the threat attempts listed in the NPRM were thwarted by intelligence efforts, not TSA screening. Other individual commenters, however, supported TSA's efforts to deploy tools like AIT scanners to detect and deter future attacks. Individual commenters credited secured cockpits and stricter policies for cockpit access with preventing terrorist attacks on commercial airlines since September 11, 2001. Furthermore, a few individual commenters suggested that in addition to enhanced cockpit security, passengers' awareness and willingness to fight back deters terrorists from targeting planes.

Several commenters discussed the evolving threat from nonmetallic explosives. A few individual commenters suggested that TSA's response to the increased threat of nonmetallic explosives is not sustainable because terrorists will find other ways to hide devices. A few individual commenters disagreed with TSA's focus on nonmetallic threats, because these types of weapons have been used for several decades.

⁶² More information on TSA Civil Rights is available at <https://www.tsa.gov/travel/passenger-support/civil-rights>.

A few individual commenters suggested that the long lines at checkpoints, which the commenters stated are caused by TSA screening, are more attractive targets to terrorists than airplanes. Lastly, several individual commenters stated there is no evidence indicating that terrorist threats similar in magnitude to September 11, 2001, are increasing.

TSA Response: TSA agrees that the threat to aviation security by terrorists continues to evolve as terrorists test current security measures to uncover vulnerabilities to exploit. Terrorist groups remain focused on attacking commercial aviation. The primary threat from these groups is from explosive devices, as we have seen in incidents originating abroad, such as the non-metallic bomb used by the Christmas Day bomber in 2009, the toner cartridge printer bombs from Yemen placed on two cargo aircraft destined for Chicago in 2011, and the improved “next generation” underwear bomb also from Yemen, recovered by a foreign intelligence service in April 2012. The incidents abroad inform us of terrorists’ intentions and capabilities, and are lessons that TSA must learn from to prevent terrorists from attempting such an act here. These examples show that terrorists continue to attack aviation, are capable of constructing non-metallic explosive devices, and continue to develop new ways to do so. Open source information indicates that terrorists continue to intend violence against aviation within the United States. TSA does not agree that intelligence reporting alone is responsible for thwarting terrorist threats. TSA agrees that improvements in intelligence gathering and sharing such information, along with other layers of security, including as mentioned in the comments, hardened cockpit doors and assistance from passengers, contribute greatly to aviation security. The combination of security layers, both seen and unseen, provides the best opportunity to detect and deter a terrorist attack.

TSA also agrees that security procedures and equipment must continue to evolve as the threat evolves. As discussed above, AIT is the most effective technology currently available to detect both metallic and nonmetallic threats, both explosive and non-explosive, concealed under passenger clothing. TSA continues to research and test new equipment and procedures to stay ahead of evolving threats.

TSA agrees that long lines at the checkpoints could pose a security risk and has taken steps to address long lines by monitoring throughput. However,

TSA remains focused on the fundamentals of security, and strives to strike a balance between security effectiveness and line efficiency. Passengers can obtain information before they leave for the airport on what items are prohibited; acceptable ID; rules for liquids, gels and aerosols; and traveling with children. Guidance for travelers with disabilities, medical conditions or medical devices, tips for dressing and packing, and information on traveling with food and gifts is provided. In addition, as noted in the NPRM, the Web site contains instructions on AIT screening procedures. 78 FR 18296. Preparing in advance for security screening and following the instructions of the TSOs are the most effective ways to reduce lines at the checkpoint.

K. TSA’s Layers of Security

Comments: Commenters addressed the TSA layers of security discussed in the NPRM. A privacy advocacy group suggested that the layered approach discussed by TSA is not supported by data and, therefore, does not justify the need for AIT. The commenter also recommended that TSA revise the layered approach so weaknesses in security can be identified. Furthermore, a few commenters suggested that TSA focus on other security methods, such as profiling, interviewing, and “Pre-check” screening programs to identify dangerous individuals. An individual stated that the efficacy of AIT screening has not been scientifically proven. The commenter further suggested that since there are other approaches used by TSA to identify potential threats, AIT would be most useful as a secondary screening method instead of as the primary screening method. A professional association, however, stated that because of the advanced methodologies of adversaries, technologies like AIT scanners are needed to secure air travel. The commenter suggested that techniques involving human intervention, such as Screening Passengers by Observation Techniques, the Behavioral Detection Officer program, and passenger screening canines would also be useful. Many commenters mentioned their support for the use of racial profiling tactics instead of AIT, and argued that such measures would be more efficient and effective.

An advocacy group alleged that TSA’s “trusted traveler program” approach would weaken security because it can eliminate entire classes of passengers from AIT screening. The commenter recommended that TSA consider other, less invasive and cost-effective screening procedures that would allow

TSA to implement AIT as a secondary, rather than a primary, screening tool. Furthermore, the commenter suggested that TSA enhance layers of security by testing canine bomb detection, face recognition, and explosives residue machines, in an effort to reduce the need for AIT scanning.

TSA Response: TSA believes that a comprehensive security system is the most effective means to address potential terrorist threats, since no single security measure may be sufficient by itself. TSA also agrees that ETD, behavior detection and passenger screening canine are valuable tools to address terrorist threats, and TSA uses these at airports.

TSA does not agree with commenters that using AIT, as a secondary screening method, would be as effective as currently deployed. Limiting its use to resolve alarms of the WTMD, which can only detect metallic threats, would severely restrict our ability to prevent adversaries from smuggling non-metallic weapons and explosives on board an aircraft.

As discussed above, AIT is the best technology currently available to detect both metallic and nonmetallic threats, and explosives as well as non-explosives. TSA has tested the effectiveness of the technology, and the equipment must meet TSA detection standards to be deployed in an airport. In addition, testing is conducted by the DHS Transportation Security Laboratory (TSL). The TSL Independent Test and Evaluation group provides certification and qualification tests and laboratory assessments on explosive detection capability. TSA procurement specifications require that any AIT system must meet certain thresholds with respect to the detection of items concealed under a person’s clothing. While the detection requirements of AIT are classified, the procurement specifications state that any approved system must be sensitive enough to detect smaller items.

Regarding the comments recommending racial profiling, transportation security screening is regulated by the Constitution, federal law, and applicable DHS and component policies setting forth the appropriate limits on use of race, ethnicity, and other characteristics. In addition, racial profiling is not an effective security measure and can easily be defeated. It is premised on the erroneous assumption that any particular individual of one race or ethnicity is more likely to engage in misconduct than any particular individual of another race or ethnicity. In addition to being ineffective,

profiling violates DHS policies and ultimately undermines the public trust. TSA disagrees with the commenter who wrote that TSA's trusted traveler program would weaken security. The TSA Pre✓™ program is based on the premise that most passengers do not pose a risk to aviation security. This program will permit those passengers who voluntarily provide information for a security risk assessment to undergo expedited screening and allow TSOs to devote more time to screening unknown passengers.

L. Effectiveness of AIT Screening

Comments: Many commenters made general statements that AIT scanners are not effective in addressing security threats. An individual commenter stated that because TSA has not released data regarding the effectiveness of AIT scanners and the number of prohibited items detected by AIT, the NPRM would not be taken seriously. Some commenters, including a privacy advocacy organization and a community organization, stated that TSA has not provided enough information about what AIT can detect. The commenter stated that the agency has not made a distinction between an "anomaly" and a "threat." Commenters also stated that the use of AIT scanners makes air travel more vulnerable to terrorism.

Many submissions discussed the efficacy of AIT to detect anomalies concealed under the clothing of a passenger. Some commenters stated that AIT scanners are not effective because they cannot detect items that are concealed under fake skin, under skin folds, or under shoes, implanted bombs, and objects hidden inside of a person. A few individuals stated that objects are not detected if concealed on the side of the body. A commenter stated that a passenger was able to bring an empty metal box concealed under clothing through AIT units without detection. The commenter believed that the metal box was not detected because the rate at which the AIT beams reflect off the metal is the same rate at which beams reflect the background. The commenter stated that if an object like the metal box were placed at the side of a body, the object beam reflection would look no different from the blackened background. According to another individual commenter, a peer-reviewed publication in the *Journal of Homeland Security* stated that explosives with low "Z" like plastics look like flesh to the scanner because flesh is also low "Z." A few individual commenters referred to a video posted by a blogger that the commenters stated portrayed a man who was able to conceal objects (both metal

and nonmetal) from an AIT scanner by sewing the objects into the lining of his shirt.

Some commenters discussed the ability of AIT to detect plastic, powder, and liquid explosives. One individual commenter stated that a 2007 government audit found that agents were able to pass through security checkpoints with explosives and bomb parts. Commenters stated that the explosives used by the "underwear bomber" and "shoe bomber" would not be detected by AIT. A commenter stated that a 2010 Government Accountability Office (GAO) report indicated that it remains unclear whether the AIT would have detected the weapon used in the December 2009 Christmas Day bomber incident based on the preliminary information GAO had received. An advocacy group also expressed concern that AIT scanners cannot detect pentaerythritol tetranitrate (the powder explosive the group states was used by the Christmas Day bomber), and claimed that this chemical continues to be used in other domestic and international terror attempts. An individual commenter alleged AIT could not detect explosives molded into specific shapes. Another individual commenter stated that since there are claims that AIT cannot detect powder explosives, AIT scanners are not fulfilling the statutory provision at 49 U.S.C. 44925 which TSA has used as justification for deploying AIT.

An individual commenter suggested that, although the AIT scanners can adequately detect metal in firearms and concealed knives, security screening should also be able to detect explosives with negligible false negative rates and low false positive rates. The commenter recommended that a reasonable detection limit would be no lower than 20 percent of the amount of the explosive needed to bring an airplane down. The commenter suggested that systems that detect significant quantities of explosives or detonators should be used for screening baggage and items concealed under clothing.

A few individuals expressed concern that because AIT on its own cannot differentiate between threatening objects and non-threatening objects, passengers carrying non-threatening objects are subject to more intrusive, secondary searches including pat-downs. A community organization stated that travelers of the Sikh religion are often subject to secondary searches even when the AIT scanner did not identify any anomalies. Similarly, an individual commenter stated that, although AIT scanners can detect anomalies, often times a pat-down could not resolve

whether the anomaly is a threat. An individual commenter, however, remarked that continued use of AIT would reduce the number of pat-downs as well as enhance detection of nonmetallic weapons, because AIT is effective in detecting threats. The commenter suggested that AIT checkpoints be re-designed to minimize the level of intrusion and embarrassment associated with scanned images.

Many commenters wrote that AIT scanners are no more effective at addressing security threats than other, less invasive screening methods. A few individual commenters and advocacy groups suggested that the NPRM has not adequately justified the ability of AIT to reduce significantly the threat of terror attacks on aircraft compared to alternative screening practices. Some individual commenters stated that the WTMD is more effective at detecting metallic items than AIT. A few of these individual commenters remarked that WTMD is as effective as AIT overall, but they preferred WTMD because it is less invasive than AIT. An advocacy group suggested that a cost-benefit analysis of AIT would certainly justify the scanners if they were effective in deterring terrorism compared to screening alternatives. An individual commenter also stated there is not enough evidence of increased threats using nonmetallic objects to justify the need for body scanners. The commenter explained that prior to AIT, nonmetallic objects were addressed by less-invasive means including WTMDs, bomb-sniffing dogs, Federal Air Marshals, and explosives detection machines. The commenter also stated that nonmetallic weapons that are small enough to conceal on the body do not pose a threat. One individual commenter, however, discussed examples where the use of the AIT scanner was instrumental in identifying weapons concealed under clothing. The commenter stated that there is no alternative technology that can assist in detecting explosives and other harmful objects that can be used to harm travelers.

Many commenters, including a non-profit organization, an advocacy group, and individual commenters, made general statements that AIT scanners are ineffective because of reported high false positive rates. An individual commenter stated that travelers might be more accepting of the invasiveness of AIT scanners if TSA revealed data regarding the effectiveness of the technology (*i.e.*, false positives and false positive rates). Several commenters, including a non-profit organization and a community organization, stated that

the false detection of non-threatening objects leads to pat-downs where passengers are subjected to unnecessary, invasive screening. An individual referenced incidents which, the commenter stated, caused passengers embarrassment when their medical device raised a false positive. An individual commenter argued that the high rate of false positives causes security checkpoint lines to move slowly, which subsequently requires TSA to use WTMDs to relieve the backup. A few individuals expressed concern regarding a false sense of security created for TSA officers and passengers by the large volume of false alarms caused by AIT scanners. The commenters concluded that this false sense of security weakens security. Similarly, an individual commenter remarked that the process of responding to false positives (searching for non-threatening objects) takes TSA's focus off identifying actual threats.

An individual commenter stated that AIT scanners are not effective in identifying a passenger with a threatening weapon because passengers can travel from airports or terminals that do not use AIT scanners. The commenter stated that passengers could also avoid detection by placing a weapon on a companion passenger under 12 years of age or on a pet. The commenter also stated that AIT scanners are ineffective at making air travel safer because the long lines make passengers more vulnerable to terror attacks. An individual commenter, however, wrote that the AIT scanners are more effective as a deterrent to terrorists than random pat-downs or profiling because of the expectation that the AIT will scan all passengers entering the sterile area.

TSA Response: TSA cannot fully address the specific detection capabilities of AIT in the final rule, because much of the information is classified. As explained in the NPRM, AIT is able to detect both metallic and nonmetallic items concealed under an individual's clothing. The NPRM describes some of the items concealed under clothing that have been detected by AIT. 78 FR 18297. AIT equipment must meet detection specifications and overall performance standards established by TSA. The AIT machines are tested regularly to ensure that the detection capabilities and performance standards are maintained. After years of testing and operational experience at the airport, TSA maintains that AIT provides the best opportunity currently available to detect both metallic and nonmetallic threats concealed under a person's clothing. TSA procurement specifications require that any AIT

system must meet certain thresholds with respect to the detection of items concealed under a person's clothing. While the detection requirements of AIT are classified, the procurement specifications require that any approved system be sensitive enough to detect smaller items. Prior to deployment, the machines are tested in the laboratory and in the field to certify that the detection standards are met. In addition, the DHS Transportation Security Laboratory (TSL) also tests the equipment to verify detection capability. After deployment, testing continues as TSA regularly conducts both overt and covert detection tests. In addition, AIT detection capability has been tested by DHS and the GAO.

The millimeter wave AIT equipment currently deployed at airports to screen passengers uses ATR software that enables the AIT automatically to identify irregularities on passengers using imaging analysis techniques based on contour, pattern, and shape. The AIT is designed to detect irregularities concealed under clothing; therefore, commenters are correct that it may detect items that do not pose a threat. Commenters also are correct that in order to determine whether AIT has alarmed on a threat item, a TSO will conduct further screening at the location where the AIT has indicated that there is an anomaly, thereby eliminating the need to pat-down the entire body. Generally, a passenger is only touched if an anomaly is indicated by AIT, and only the part of the body where the machine has indicated an anomaly is located is touched during the pat-down. At times, ETD or other forms of additional screening may be employed to resolve an alarm and to clear a passenger for entry into the sterile area after AIT screening. Passengers are advised to avoid wearing clothing with large metal embellishments and large metal jewelry and to remove all items in their pockets to reduce the possibility that the AIT will alarm on innocuous items.

TSA is aware of the audits conducted by the GAO on the effectiveness of screening measures. However, AIT was not in use at the checkpoint when the GAO tested security procedures described in the 2007 report cited by a commenter.⁶³ The 2010 report cited by a commenter did not contain any recommendations regarding the use of AIT, but did state that a cost/benefit

⁶³ U.S. Government Accountability Office, "Aviation Security Vulnerabilities Exposed Through Covert Testing of TSA's Passenger Screening Process," GAO-08-48T (Nov. 15, 2007).

analysis would be beneficial.⁶⁴ The RIA includes an extensive analysis of the costs of AIT and a qualitative discussion of its benefits. In addition, the RIA discusses the alternatives to AIT considered by TSA.

TSA disagrees with the comments alleging that because there is no direct evidence that AIT has prevented a terrorist attack on its own, the technology is not effective. As the Supreme Court pointed out in rejecting a similar argument in *Von Raab*, the validity of a screening program does not turn on "whether significant numbers of putative air pirates are actually discovered by the searches conducted under the program." Given the government's interest "in deterring highly hazardous conduct," the Supreme Court emphasized, "a low incidence of such conduct, far from impugning the validity of the scheme . . . is more logically viewed as a hallmark of success." 489 U.S. at 675 n.3.⁶⁵ In *Corbett*, the Court of Appeals upheld the use of AIT and found that "the scanners effectively reduce the risk of air terrorism . . . the Fourth Amendment does not require that a suspicionless search be fool-proof or yield exacting results."⁶⁶

Further, the fact that AIT, or any single security measure, may not be completely foolproof does not mean that it is ineffective and should not be used at all. A discussion of the alternatives to AIT considered by TSA is included in the RIA. TSA has always maintained that AIT is the best technology currently available to detect the threat of nonmetallic and other dangerous items and that a comprehensive security system is the best means to detect and deter terrorist attacks as no single layer by itself, including AIT, may be sufficient. Accordingly, TSA agrees with commenters that other security measures, including those mentioned in the comments such as canine, Federal Air Marshalls, and explosive detection systems, should also be deployed to increase the chance that a threat will be detected. TSA does in fact employ all of those measures. However, TSA does not

⁶⁴ U.S. Government Accountability Office, "Aviation Security TSA is Increasing Procurement and Deployment of the Advanced Imaging Technology, but Challenges to This Effort and Other Areas of Aviation Security Remain," GAO-10-484T (Mar. 17, 2010).

⁶⁵ See also *MacWade v. Kelly*, 460 F.3d 260, 274 (2d Cir. 2006) (holding that the deterrent effect of an anti-terrorism screening program in the New York subway system "need not be reduced to a quotient" to satisfy 4th Amendment balancing.) and *Cassidy v. Chertoff*, 471 F.3d 67, 83 (2d Cir. 2006) (government is not required to "adduce a specific threat" to ferry system before engaging in suspicionless searches).

⁶⁶ *Corbett*, 767 F.3d at 1181.

agree that any of those measures should replace AIT because AIT provides stand-alone value as well.

In response to a comment regarding the redesign of the checkpoint to minimize embarrassment of passengers during the screening process, TSA points out that since May 2013, TSA has only deployed AIT with ATR software at the airport. ATR eliminates the individual image and produces a generic outline that is visible to the passenger and the TSO. In addition, TSA offers passengers who must undergo a pat-down the opportunity to have the pat-down conducted in a private screening location that is not visible to the traveling public.

Currently there are approximately 793 AIT machines located at almost 157 airports nationwide. Given limited resources, TSA uses a risk-based approach to deploy AIT and continues to assess and test “next generation” AIT systems, which TSA anticipates will improve anomaly detection capability, decrease processing time, and better suit the physical constraints of airport checkpoints.

M. Screening Measures Used in Other Countries

Comments: Commenters discussed screening measures used in foreign countries. The majority of these comments recommended that TSA consider implementing a screening system similar to the one used by Israel. In addition to individual commenters, a privacy advocacy group stated that in 2011 the European Union (EU) issued a ruling banning the use of backscatter body scanners in all airports; that Italy discontinued its use of millimeter wave scanners because they were found to be slow and ineffective; and that Germany and Ireland discontinued use of AIT because of concerns regarding efficacy. A few individual commenters stated that the AIT scanners were removed from other countries because of health and safety concerns.

TSA Response: AIT is used in airports and mass transit systems in many countries, including in Canada, the Netherlands, Australia, Nigeria, and the United Kingdom.⁶⁷ TSA works directly with foreign governments and through the International Civil Aviation Organization (ICAO) to share information on AIT as well as other security measures.⁶⁸ TSA continues to

believe that AIT provides the most effective technology currently available to detect metallic and nonmetallic threats. As was explained in the NPRM and discussed below, AIT has been tested for safety by both TSA and independent entities. The results confirm that AIT is safe for individuals being screened, equipment operators, and bystanders. See 78 FR 18294–18296.

TSA is aware that the European Commission adopted a legal framework on security scanners.⁶⁹ That framework states that the use of security scanners is optional, and that only security scanners which do not use ionizing radiation can be deployed and used for passenger screening. It also specifies that the scanners shall not store, retain, copy, print, or retrieve images. However, the Commission also found that “[s]ecurity scanners are an effective method of screening passengers as they are capable of detecting both metallic and non-metallic items carried on a person. The scanner technology is developing rapidly and has the potential to significantly reduce the need for manual searches (“pat downs”) applied to passengers, crews and airport staff.”⁷⁰

N. Laboratory and Operational Testing of AIT Equipment

Comments: Some submissions discussed testing of AIT scanners for operational effectiveness. Several commenters stated that no testing has been conducted by independent parties, or they expressed concern that TSA did not publicly release the results of AIT equipment testing. A few individual commenters objected to having TSA test the scanners on the traveling public. An individual commenter suggested that validation tests should include evidence of attempts to defeat a screening technique and recommended that if the results indicate that AIT is less effective for screening than other devices, TSA should discontinue use of AIT in favor of technology that the results favor.

An individual commenter stated the need for long-term studies, including potential effects of the AIT equipment if it were to malfunction, become “out of spec,” or suffer from poor maintenance.

TSA Response: The FAA began testing AIT when it was responsible for

passenger screening at airports prior to the creation of TSA. TSA continued laboratory testing of AIT as the threat from nonmetallic substances increased. To better assess the application of AIT to the airport environment, TSA conducted limited field trials of different types of AIT equipment at several airports. Throughout 2007 and 2008, AIT was piloted in the secondary position for these trials. In 2009, in response to the Christmas Day bomber, TSA began to evaluate using AIT in the primary screening position since there are no other currently deployed technologies in the primary screening position that can detect nonmetallic threats concealed under a passenger's clothing. When conducting tests both in the laboratory and in the field, TSA evaluated the equipment for safety, detection capability, operational efficiency, and passenger impact. Because of the successful results observed during testing and the need to address the threat from nonmetallic explosives concealed under clothing, TSA decided to procure AIT units for use in the primary position at airport checkpoints.

All of the AIT units are regularly inspected by the manufacturer to ensure that they operate effectively and meet TSA specifications. In addition, the units are tested each day prior to use at the checkpoint. If the equipment does not meet operational specifications, it cannot be used.

The GAO released a report, “Advanced Imaging Technology: TSA Needs Additional Information before Procuring Next-Generation Systems,” in March 2014 describing the types of tests TSA conducts on AIT.⁷¹ As explained in the report, TSA conducts the following five tests to evaluate the performance of AIT equipment: (1) Qualification testing in a laboratory setting at the TSA Systems Integration Facility to evaluate the technology's capabilities against TSA's procurement specification and detection standard to include testing of false alarm rates; (2) Operational testing at airports to evaluate system effectiveness and suitability for the airport environment; (3) Covert testing to identify vulnerabilities in the technology, operator use, and TSO compliance with procedures; (4) Performance Assessments to test TSO compliance with Standard Operating Procedures (SOPs); and (5) Checkpoint drills to assess TSO compliance with SOPs and ability to resolve anomalies

⁶⁷ <http://science.howstuffworks.com/millimeter-wave-scanner4.htm>; <http://cnsnews.com/news/article/us-paid-full-body-scanners-nigeria-s-four-international-airports-2007>.

⁶⁸ ICAO recognizes that AIT may be used as a primary screening measure for passengers. ICAO

“Aviation Security Manual,” Doc 8973/8 Restricted (2011).

⁶⁹ European Commission, Press Release, “Aviation Security: Commission Adopts New Rules on the Use of Security Scanners at European Airports,” Brussels, Belgium (Nov. 14, 2011). The countries referenced by several commenters (Germany, Ireland, and Italy) are members of the European Union.

⁷⁰ *Id.*

⁷¹ U.S. Government Accountability Office Report to Congressional Requesters, “Advanced Imaging Technology: TSA Needs Additional Information before Procuring Next-Generation Systems,” GAO-14-357, March 2014.

identified by AIT.⁷² Qualification testing is conducted when a technology is first considered for deployment and for subsequent upgrades to the technology. The TSL also conducts certification testing on detection capability. In addition to these tests, the actual units are subjected to a factory acceptance test at the manufacturer's facility and a site acceptance test at the airport. TSA also tests the units for radiation exposure as described in the NPRM and in response to additional comments described below. Covert testing is also conducted by the Inspector General of DHS and GAO.⁷³ TSA studies the results of laboratory and covert tests closely, and modifies procedures as appropriate. TSA believes that the testing described above adequately supports the use of AIT as a primary screening mechanism.

O. Radiation Exposure

Comments: The effects of radiation associated with AIT use was also addressed by commenters. A professional association stated its belief that AIT emissions present a negligible health risk to passengers, airline crewmembers, airport employees, and TSA staff. Numerous commenters, however, expressed concern regarding exposure to radiation. Some of these commenters suggested that no dose of radiation is safe. Many individual commenters and an advocacy group expressed concern about the radiation from backscatter scanners, which they stated could lead to the development of cancer. Many individuals also warned that exposure to millimeter wave radiation could hold the potential for long-term health effects and that additional studies are needed. Some commenters concluded that, even if the

current x-ray scanners were removed, the proposed rule would not prevent their reintroduction should software become available to address privacy issues.

Several commenters, including a privacy advocacy organization, a non-profit organization, and individual commenters, cautioned that TSA screeners could be at risk and should be provided with dosimeters to ensure that their exposure is within acceptable limits. An individual commenter stated that, although TSA claimed that the radiation scan only affects the surface of the skin, skin cancer is the largest incidence of cancer in the world, and it is caused by radiation exposure on the skin. Another commenter stated that eyes are particularly susceptible to radiation. A few individuals suggested that imaging technology using radiation should not be used at all since alternatives exist. Other commenters stated that the question that needs to be asked with respect to the safety of AIT scanning is not whether the increase in deaths is below some arbitrary value, but whether the lives saved through avoiding a terrorist attack are greater than the lives lost through an increased incidence of cancer or other diseases arising from the use of AIT scanners. Lastly, a few individuals mentioned that because of their exposure to radiation for medical treatment, they are not comfortable getting further, unnecessary exposure from AIT scanners.

TSA Response: In compliance with the statutory requirement that all AIT machines used for screening be equipped with and employ ATR software, TSA removed the general-use backscatter AIT units from the checkpoint.⁷⁴ TSA notes that it is adopting the statutory requirement mandating the use of ATR software on AIT used to conduct screening in the regulatory text.

Contrary to assertions by some commenters and as discussed in the NPRM, general-use backscatter units were independently evaluated and found to be within national standards for acceptable radiation exposure by the Food and Drug Administration (FDA)'s Center for Devices and Radiological Health (CDRH), the National Institute of Standards and Technology, the Johns Hopkins University Applied Physics Laboratory and the U.S. Army Public Health Command.⁷⁵ A report issued by the DHS Office of Inspector General in 2012 confirms that prior to the deployment of general-use backscatter

units, TSA conducted four radiation safety assessments and the results of each study concluded that the level of radiation emitted was below ANSI's acceptable limits.⁷⁶

In addition, in June 2013, the American Association of Physicists in Medicine released the results of an independent study of the general-use backscatter units previously used by TSA for screening passengers.⁷⁷ The study measured exposures across multiple scanners in both the factory and in real-time use at airports, including organ doses. This study also found that radiation doses were below the ionizing radiation limits set by the American National Standards Institute and Health Physics Society (ANSI/HPS) and were safe for employees and passengers, including children, pregnant women, frequent flyers and individuals with medical implants.

In the NPRM, TSA noted that DHS had requested the National Academies of Sciences, Engineering, and Medicine to review previous studies as well as current processes to estimate radiation exposure resulting from the general-use backscatter equipment. That study was released in October 2015 and confirms that radiation doses did not exceed the ANSI/HPS standard.⁷⁸

As explained in the NPRM, the ANSI/HPS standard takes into consideration individuals who may be more susceptible to radiation health effects, such as pregnant women, children, and persons who receive radiation treatments, as well as the general exposure to ionizing radiation present in the environment. 78 FR 18295. In fact, the radiation emissions from the general-use backscatter equipment were so low that they were below the environmental radiation emissions that individuals are exposed to every day, and individuals would have to be screened more than 200 times a year to exceed the negligible individual dose, which is still below the ANSI/HPS standard.⁷⁹ 78 FR 18296.

⁷⁶ Department of Homeland Security, Office of Inspector General, "Transportation Security Administration's Use of Backscatter Units," OIG-12-38, Feb. 2012 at p. 5.

⁷⁷ "Radiation Dose from Airport Scanners," American Association of Physicists in Medicine, AAPM Report No. 217 (2013). Available at <http://www.aapm.org/pubs/reports>.

⁷⁸ National Academies of Sciences, Engineering, and Medicine. Airport Passenger Screening Using Backscatter X-Ray Machines: Compliance with Standards (2015), available at <http://www.nap.edu/21710>.

⁷⁹ TSA disagrees with the comments that attempted to link AIT to skin cancer, for the reasons explained in this preamble. TSA notes that according to the Stanford Medicine Cancer Institute, ultraviolet radiation from the sun is the

Continued

⁷² The report also contained recommendations to improve TSO performance on AIT and resource effectiveness, and to ensure that next generation AIT units meet mission needs. TSA generally concurred in the recommendations and noted that it will review its screening assessment programs, monitor, update and report efforts to capture operational data on screening, improve its assessment of overall effectiveness of next-generation AIT and complete a more comprehensive technology roadmap.

⁷³ The Inspector General of DHS recently conducted covert testing of TSA aviation security screening and the Secretary has directed TSA to undertake a number of steps to enhance security capabilities and techniques. See, e.g., Statement by Secretary Jeh C. Johnson On Inspector General Findings on TSA Security Screening, Press Release, Jun. 1, 2015. TSA's response to the Inspector General's findings and the changes TSA has implemented to address those findings were discussed in the testimony of TSA Administrator, Peter V. Neffenger, before the Senate Committee on Appropriations, Subcommittee on Homeland Security on Sep. 29, 2015. See <https://www.tsa.gov/news/testimony/2015/09/29/testimony-tsa-efforts-address-oig-findings>.

⁷⁴ 49 U.S.C. 44901(l).

⁷⁵ 78 FR 18295. See also <https://www.tsa.gov/FOIA>.

As explained in the NPRM, the millimeter wave equipment uses non-ionizing radio frequency energy. 78 FR 18294–18295. The millimeter wave equipment used by TSA must comply with the 2005 Institute of Electrical and Electronics Engineers, Inc. Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields (IEEE Std. C95.1™—2005) as well as the International Commission on Non-Ionizing Radiation Protection Guidelines for Limiting Exposure to Time-Varying Electric, Magnetic, and Electromagnetic Fields, Health Physics 74(4); 494–522, published April 1998. The equipment also is consistent with Federal Communications Commission and Health Canada Safety Code regulations. 78 FR 18295. The FDA confirmed that millimeter wave security systems that comply with the IEEE Std. C95.1™—2005 cause no known health effects.⁸⁰ TSA has posted a compilation of emission safety reports of the millimeter wave technology system.⁸¹

TSA implemented safety protocols to ensure that AIT is safe for passengers and the TSA workforce. When backscatter machines were still in use, each individual AIT machine was tested once a year to verify that radiation emitted fell within the national safety standards. Regular testing is also conducted on checkpoint machines that use x-ray technology, such as baggage scanners. This testing is performed by the manufacturers or maintenance providers in accordance with their TSA contracts. Because of the regular testing of TSA equipment, there is no need for operators to wear dosimeters to measure radiation emissions. In the event that a radiation test was to reveal that the emission was above the standard, the machine would be immediately taken out of service and TSA would conduct a system-wide review.

P. Other Health and Safety Issues

Comments: Commenters also mentioned other safety and health concerns related to AIT. Numerous individual commenters generally stated that they consider the safety of the AIT scanners to be uncertain and that they are concerned that AIT is harmful to

their health. Some individuals suggested that the machines amount to a medical examination performed by someone who is not a trained medical professional. A few individual commenters expressed concern about the maintenance and calibration of the scanners. According to another individual commenter, the AIT scanners and pat-downs are a physical and psychological attack on an individual, and the passenger must restrain himself or herself from natural instincts to move away from harmful physical contact to ensure their privacy and to avoid health risks.

TSA Response: All AIT units are tested for safety, detection capability, operational efficiency, and impact on passengers prior to deployment. The millimeter wave units currently in use at the airports do not use ionizing radiation. Federal law requires that all AIT units be equipped with ATR software, which does not produce an individual image, only a generic outline that is visible on the machine. TSA permits passengers generally to opt out of AIT screening and receive a thorough pat-down instead. TSA has also instituted the TSA Pre✓™ program, which allows known and trusted travelers an opportunity to undergo expedited screening, which sometimes includes screening by WTMD. This program increases throughput (among other changes) and improves the screening experience of frequent, trusted travelers. Of course, in order to maintain comparable security, no passenger is guaranteed expedited screening, and program participants may be required to undergo regular screening on a random basis.

Q. Backscatter Technology

Comments: Some submissions specifically addressed backscatter technology. Many individual commenters opposed the use of backscatter technology because of the alleged health impact. According to several commenters, x-ray radiation is cumulative, and the effects over a lifetime are not well known. A few individual commenters added that the people who may be most at risk are TSA personnel working near the scanners and frequent flyers, who are already exposed to radiation from high altitude flying. In addition, another individual commenter suggested that, even if the risk to one individual is small, when the machines are used on hundreds of millions of people, the probability that some set of individuals acquire cancer is significant.

One commenter warned that ionizing radiation might cause deoxyribonucleic

acid (DNA) damage that leads to carcinogenesis and that a model used by the health physics community would predict the probability of a fatal cancer about the same as the probability of being killed by a terrorist in an airplane. However, the commenter expressed the belief that the real danger is very high local radiation exposures if the mechanical scanning mechanism and associated systems for shutting off the x-ray beam fail. Another individual disputed TSA's statement that independent tests had been conducted on backscatter technology, and the commenter stated that subsequent information showed that the tests were flawed, their results were misused, or they were not conducted by truly independent entities.

A few commenters, including an individual commenter and a privacy advocacy group, remarked on the ineffectiveness of backscatter machines. One of them suggested that the x-ray beam might not be able to distinguish between explosives and tissue when an explosive package is shaped to fit in with natural body contours. An individual commenter stated that even though TSA is removing backscatter scanners from airports, until the process is complete, they would continue to be used at some airports. Another individual recommended that TSA investigate the bad management decision that led to a waste of tax dollars on what the commenter described as an obviously unacceptable technology. Another commenter suggested that backscatter technology was adopted because of lobbying by politically connected individuals with a financial interest in the machines. A few commenters discussed TSA's selection to use Rapiscan as the vendor for AIT scanners. According to some individual commenters, the choice of using Rapiscan as the vendor is inappropriate because a former DHS Secretary was reported to have lobbied for Rapiscan and AIT prior to his departure from the agency.

TSA Response: As discussed above, the general-use backscatter AIT equipment deployed by TSA was tested for safety, detection capability, operational efficiency, and passenger impact before deployment.⁸² Independent testing confirmed that the x-ray emissions from the general-use backscatter units were so low as to

main cause of skin cancer. <http://stanfordhealthcare.org/medical-conditions/cancer/skin-cancer/causes-skin-cancer/ultraviolet-radiation.html>. There is no evidence that AIT is related to the incidence of skin cancer.

⁸⁰ FDA, "Products for Security Screening of People," available at <http://www.fda.gov/Radiation-EmittingProducts/RadiationEmittingProductsandProcedures/SecuritySystems/ucm227201.htm>.

⁸¹ <https://www.tsa.gov/FOIA>.

⁸² All general-use backscatter AIT units were removed from screening checkpoints as of May 16, 2013, to comply with the statutory requirement that any AIT used to screen passengers be equipped with and employ ATR software. 49 U.S.C. 44901(l). The backscatter AIT units in use at the time were unable to employ ATR software.

present a negligible risk to passengers, airline crew, airport employees, and TSA employees. 78 FR 18294–18296. Any future backscatter AIT units would also be tested to ensure compliance with applicable safety standards.

Regarding the marginal effects of x-ray radiation, as TSA noted in the NPRM, 78 FR 18295–18296, the ANSI/HPS standard reflects the standard for a negligible individual dose of radiation established by the National Council on Radiation Protection and Measurements at 10 microsieverts per year. Efforts to reduce radiation exposure below the negligible individual dose are not warranted because the risks associated with that level of exposure are so small as to be indistinguishable from the risks attendant to environmental radiation that individuals are exposed to every day. The level of radiation emitted by the Rapiscan Secure 1000 is so low that most passengers would not have exceeded even the negligible individual dose. The European Commission released a report conducted by the Scientific Committee on Emerging and Newly Identified Health Risks on the risks related to the use of security scanners for passenger screening that use ionizing radiation such as the general-use backscatter AIT machines.⁸³ The health effects of ionizing radiation include short-term effects occurring as tissue damage. Such deterministic effects cannot result from the doses delivered by security scanners. In the long term, it found that the potential cancer risk cannot be estimated, but is likely to remain so low that it cannot be distinguished from the effects of other exposures including both ionizing radiation from other natural sources, and background risk due to other factors.

Regarding commenters' concerns that ionizing radiation might cause deoxyribonucleic acid (DNA) damage, as TSA noted in the NPRM, the annual dose limits in ANSI/HPS N43.17 are based on dose limit recommendations for the general public published by the National Council on Radiation Protection and Measurements in Report 116, "Limitations of Exposure to Ionizing Radiation." The dose limits were set with consideration given to individuals, such as pregnant women, children, and persons who receive

radiation treatments, who may be more susceptible to radiation health effects. Further, the standard also takes into consideration the fact that individuals are continuously exposed to ionizing radiation from the environment. ANSI/HPS N43.17 sets the maximum permissible dose of ionizing radiation from a general-use system per security screening at 0.25 microsieverts. The standard also requires that individuals should not receive 250 microsieverts or more from a general-use x-ray security screening system in a year.

Regarding comments about whether AIT can distinguish between explosives and tissue when an explosive package is shaped to fit in with natural body contours, the AIT equipment is designed and tested to find such items.

Regarding comments about the procurement of backscatter technology and Rapiscan, all TSA acquisitions were in compliance with Federal procurement standards. TSA issued a competitive solicitation for companies to submit AIT machines for qualification testing, and while competitive pricing was submitted by two vendors, only Rapiscan was qualified and placed on the Qualified Product List before the planned award date of September 2009. The award was then made to Rapiscan for the initial order.

R. Millimeter Wave Technology

Comments: Some submissions specifically addressed millimeter technology. Many commenters, including individual commenters and non-profit organizations, stated that although TSA claims that millimeter wave scanners are safe, they were unconvinced. Several of these commenters stated TSA had not conducted long-term, independent testing of millimeter wave equipment. Others noted that the scanners still emit a form of radiation and may be harmful. A non-profit organization added that babies, small children, pregnant women, the elderly, and people with impaired immunity would be at a higher risk from non-ionizing radiation than others would. An individual commenter remarked that studies have shown a trend toward higher rates of brain and other tumors in those who use cell phones, which produce a similar form of non-ionizing radiation. Two other individuals suggested that millimeter wave exposure could be harmful to human DNA because of resonance effects.

Although some commenters supported the use of millimeter wave technology over backscatter technology, an individual and an advocacy

organization stated they were disinclined to take the government at its word with regard to health assurances because the government has been wrong before, including TSA assurances about Rapiscan machines. An individual commenter stated that millimeter wave machines are no more acceptable than other scanners, but those who must fly will choose them to avoid a pat-down.

One individual commenter recommended another technology for detecting explosives—passive Terahertz (THz) imaging. According to the commenter, there would be no probing radiation, but the warm body emits sufficient THz radiation to form an image, with high explosives standing out in the image as a dark patch.

TSA Response: As discussed in the NPRM, millimeter wave imaging technology used by TSA to screen passengers meets all known national and international health and safety standards. 78 FR 18295. Millimeter wave units are tested for electromagnetic emissions prior to acceptance. The FDA examined the exposure to non-ionizing electromagnetic energy and found that the short duration of screening, approximately 1.5 seconds, and the very low levels of emissions showed that the energy emitted by millimeter wave technology systems is approximately a thousand times less than the limit set by the Institute of Electrical and Electronics Engineers (IEEE). FDA evaluated the Millimeter Wave AIT to determine if the RF emissions met the safety levels established for the general public in C95.1–2005. The exposure a person receives during one scan at a worst-case distance of 10 cm from the inner wall of the unit is on the order of 1000 times less than the IEEE standard's limit for the public exposure. IEEE Std 95.1 defines general public as "individuals of all ages and varying health status . . . Generally, unless specifically provided for as part of an RF safety program, the general public includes, but is not limited to, children, pregnant women, individuals with impaired thermoregulatory systems, individuals equipped with electronic medical devices, and persons using medications that may result in poor thermoregulatory system performance." [IEEE Std 95.1–2005, page 7, 3.1.26]. TSA has posted a report on its Web site that includes the evaluation performed by the FDA.⁸⁴

⁸³ The SCENIHR is an independent committee that provides the European Commission with the scientific advice it needs when preparing policy and proposals relating to consumer safety, public health, and the environment. The committee is made up of external experts. See SCENIHR (Scientific Committee on Emerging and Newly Identified Health Risks), Health effects of security scanners for passenger screening (based on X-ray technology), 26 April 2012.

⁸⁴ "Compilation of Emission Safety Reports on the L3 Communications, Inc. ProVision 1000 Active Millimeter Wave Advanced Imaging Technology (AIT) System," Sept. 2012. See, www.dhs.gov/advanced-imaging-technology-documents.

TSA is aware of the paper cited by commenters that reportedly found that THz radiation could affect biological function, but only under specific conditions and extended exposure. The paper, "DNA Breathing Dynamics in the Presence of a Terahertz Field," was published by scientists from the Theoretical Division and Center for Nonlinear Studies at Los Alamos National Laboratory in 2010. The millimeter wave machines deployed by TSA do not operate in the THz range, or at the power level referenced in the paper, and the exposure time for passengers screened by AIT is approximately 1,000 times less than the exposure time referenced in the paper.

TSA has evaluated other technologies to assess whether they are safe, meet all applicable government and industry standards, are effective against known and anticipated threats, and require the least disruption and intrusion on passenger privacy possible. For example, TSA has tested passive THz systems in the past and found that they were not effective in detecting explosive threats in an airport environment. Likewise, TSA considered Infrared technology but found that detection capability and operational effectiveness were limited. However, TSA continues to research and assess engineering developments and new technologies for use in the airport.

S. Concerns Regarding Privacy

Comments: Many submissions addressed concerns related to privacy. Many individual commenters, a non-profit organization, and advocacy groups expressed the opinion that the devices should be called "Nude Body Scanners" or "Naked Body Scanners" to indicate specifically how TSA uses them, and other commenters preferred "Electronic Strip Searches" or "virtual strip searches" or "nude-o-scopes." Numerous individuals insisted that AIT scanners violate an individual's right to privacy, that TSA's privacy safeguards are inadequate, and that the scanners should not be used on children. Some commenters stated that if scanners are viewing anything under a person's clothing, then that person's privacy is not being protected, because anything under the clothing is intentionally hidden and not meant to be viewed by man or machine. An advocacy group agreed that AIT defeats the privacy-protecting function of clothing and allows an image of the unclothed person to be created. An individual commenter remarked that the problem with TSA's use of AIT for primary screening is it teaches people it is normal and acceptable for the government to use

technology to look under their clothing. The commenter added that the body beneath one's clothing and the contents of one's pockets traditionally have been understood as among the most important and intimate zones of privacy.

One commenter noted that passengers must reveal private medical conditions to TSA officers who are not trained in medicine, and others stated that investigating private details of passengers' bodies is deeply offensive and has no security value. A community organization agreed that privacy is invaded when a passenger is forced to share personal secrets that are not otherwise observable in public—especially sensitive medical and gender identity issues. One commenter, however, expressed the opinion that over the years, TSA staff has become more respectful of individual passenger privacy.

A privacy advocacy group pointed out that since January 2008, TSA has published four Privacy Impact Assessments (PIAs) regarding the agency's deployment of body scanners at U.S. airports. The commenter opined that all of these have failed to identify the numerous privacy risks to air travelers. An individual commenter suggested that TSA should be required to regularly report to Congress about its efforts to discover weaknesses in its mechanisms to protect the privacy of individuals scanned by its systems.

Some submissions suggested other technologies and procedures for safeguarding privacy. Among the procedures recommended by one individual were: (1) Providing a generic image of all scanned passengers and (2) allowing a person to leave if selected for a manual search, provided the person exhibits no other suspicious behavior. One commenter suggested that if the AIT screening procedures detect potentially dangerous objects hidden in passengers' private areas, the passengers should be allowed to remove the suspicious objects, show them to TSA officers, and be rescreened using AIT. Another individual suggested developing technology to combat scanner fatigue, providing oversight in screening rooms, and addressing the threat of privacy or security breaches when the status of a passenger is relayed by two-way radio.

TSA Response: As stated previously, Federal law requires that all AIT equipment used to screen passengers must be equipped with and employ the use of ATR. The ATR software produces a generic outline that is publicly displayed on the equipment. The use of ATR mitigates privacy concerns because

there is no individual image of a passenger's body, only a generic outline that is the same for passengers based on gender. The AIT equipment used by TSA is not able to store, transmit, or print any images. After each passenger is screened using the AIT, the TSO clears the generic outline of any alarms so that the next passenger may be screened. Signs are posted at the checkpoint and information is available on TSA's Web site showing a sample of the ATR generic outline and advising passengers that they may decline AIT and receive a thorough pat-down. The court in *Corbett* found that the "scanners pose only a slight intrusion on an individual's privacy, especially in the light of the automated target recognition software installed in every scanner. The scanners now create only a generic outline of an individual, which greatly diminishes any invasion of privacy."⁸⁵

TSA has posted information on AIT technologies and ATR on its Web site, and published a PIA in January 2008 with subsequent updates. TSA also conducted outreach with national press and privacy advocacy groups to discuss AIT. While most PIAs are required on information systems that collect information in identifiable form, which AIT does not, DHS nevertheless conducted PIAs on TSA's use of AIT. As explained in the PIA, "the operating protocols of remote viewing for AIT machines that were not equipped with ATR software, coupled with no image retention, are strong privacy protections . . . ATR software provides even greater privacy protections by eliminating the human image . . ."⁸⁶

TSA disagrees with the alternate procedures suggested by some of the commenters. Federal courts have upheld TSA's procedure to require passengers to complete the screening process once it has been initiated by the passenger. As the U.S. Court of Appeals for the Ninth Circuit explained in *Aukai*,

The constitutionality of an airport search, however, does not depend on consent . . . and requiring that a potential passenger be allowed to revoke consent to an ongoing airport security search makes little sense in a post-9/11 world. Such a rule would afford terrorists multiple opportunities to attempt to penetrate airport security by 'electing not to fly' on the cusp of detection until a vulnerable portal is found. This rule would also allow terrorists a low-cost method of detecting systematic vulnerabilities in airport

⁸⁵ *Corbett*, 767 F.3d at 1181.

⁸⁶ Privacy Impact Assessment Update for TSA Advanced Imaging Technology, Jan. 25, 2011, www.dhs.gov/xlibrary/assets/privacy/privacy-pia-tsa-ait.pdf.

security, knowledge that could be extremely valuable in planning future attacks.

U.S. v. Aukai, 497 F.3d 955, 960–61 (9th Cir. 2007) (en banc) (internal citations omitted). Finally, TSA's procedures permit passengers generally to opt out of AIT screening and receive a thorough pat-down instead, which may be conducted in private and in the presence of a companion of the passenger's choosing.

T. Use of ATR Software

Comments: Some submissions discussed TSA's use of ATR software. Numerous submissions from individual commenters remarked that even though ATR software displays a generic outline on the screen at the checkpoint, ATR does not eliminate air travelers' privacy concerns. Many of these commenters, including individuals and advocacy groups, expressed opposition to the use of ATR because, according to the commenters, ATR can be disabled and the scanners are capable of producing explicit, nude pictures that may be viewed by TSA staff. Individual commenters and an advocacy group stated that ATR does not alleviate concerns about the intrusiveness of scanning, its ineffectiveness, the violation of privacy, and possible health effects. A few individuals and a professional association, however, expressed support for the use of ATR because the technology helps mitigate passengers' privacy concerns. An individual commenter stated that TSA took a year longer than legally allowed to cease use of AIT scanners without ATR software.

TSA Response: TSA's deployment of ATR software was completed in accordance with Federal law and before the established deadline. TSA agrees with commenters that the use of ATR software addresses privacy concerns since there is no individual image, and there is no need for a TSO to view an individual image. In addition, TSA believes that the ATR detection capability is commensurate to that of a TSO review and is likely faster, thereby decreasing the amount of time passengers must spend at the checkpoint. TSOs are not able to disable the software, and each AIT unit is delivered to the airport with software that precludes placing the unit into a mode that would allow TSOs to obtain unfiltered, passenger-specific images. Further, the equipment cannot store, transmit, or print individual images, and TSOs are not able to install or activate any such capability on the equipment.

U. Protection of Images

Comments: Commenters also addressed the issue of image protection controls. Numerous individual commenters suggested that they were not convinced by TSA's assertions regarding image protection. Several individual commenters mentioned reports of incidents involving recorded and leaked images from scanners, such as the reported release of 35,000 images created by a Rapiscan machine at a courthouse in Florida. Other individuals and advocacy groups warned that because the scanners have the capability to store and transmit images, at least some storage of images by TSA and viewing by others is likely. Some of these commenters alleged that TSA had falsely stated that previous imaging machines could not store, transmit, or print images.

A privacy advocacy group pointed out that the scanners were designed to include Ethernet connectivity, Universal Serial Bus access, and hard disk storage, but the proposed rule does not include safeguards against storing, copying, or otherwise circulating images. An advocacy group added that the scanners are worse than a physical strip-search because they produce an image that can be stored indefinitely, transferred around the globe in seconds, and copied an infinite number of times without the copies degrading. According to an individual commenter, law enforcement officers can record images without the passenger's knowledge. Some commenters, including individuals and a privacy advocacy association, recommended that TSA clarify what happens to the images captured, who gets to see them, and whether the practice of deleting the image after each screening is absolute. A couple of individual commenters also suggested that TSA should show the public exactly how detailed the image seen in the screening room is, or allow passengers being scanned to observe the personnel monitoring the images. A few individuals, however, expressed support for TSA's efforts to protect passenger privacy by ensuring that the images are anonymous and are automatically deleted from the system after the remotely located security officer clears them.

TSA Response: Federal law requires that all AIT equipment used to screen passengers be equipped with and employ ATR. TSA removed all AIT equipment that could not use ATR software by May 16, 2013, in advance of the statutory deadline. The ATR software does not produce an individual image but instead produces a generic

outline that is publicly displayed on the equipment. A picture of the generic outline is posted at the checkpoint and on TSA's public Web site.⁸⁷ Consequently, the individual image has been eliminated and there is no longer any need for a TSO in a remote location to view the image.

Initial versions of AIT were manufactured with storage and transmittal functions that TSA required manufacturers to disable prior to installation at airports. TSA confirmed that these functions were disabled during factory acceptance testing and site acceptance testing. The TSOs were not able to activate the functions. As explained in the NPRM, images were transmitted securely between the unit and the viewing room so they could not be lost, modified, or disclosed.⁸⁸ The images produced were encrypted during this transmission and were completely deleted in the viewing room once the individual was cleared. The TSO in the viewing room was prohibited from bringing electronic devices such as cameras, cell phones or other recording devices into the viewing room. Violations of these procedures would subject the TSO to disciplinary action, up to and including termination. Note that the current versions of AIT do not have the capability to create an image; rather, they create internal code of the passenger using proprietary software that it analyzes and uses to show an alarm box on the generic outline, if appropriate.

The AIT devices at airports do not have the ability to transmit, store, or print images. While use of AIT in other locations, such as courthouses, was discussed in the comments, TSA does not operate AIT in those locations. AIT that is equipped with ATR software does not produce an individual image; even prior to the use of ATR, TSA's privacy safeguards, detailed in the NPRM, would have prevented the production, let alone release, of images described in the comments.⁸⁹

V. Conducting a Pat-Down as the Alternative to AIT

Comments: Comments also addressed the use of the pat-down as the alternative to AIT. Many individual commenters and an advocacy group stressed the importance of having TSA retain the option to undergo a pat-down instead of AIT; although some pointed out that many passengers select the pat-down over AIT only because they consider it the lesser of two evils. Many

⁸⁷ <https://www.tsa.gov/travel/travel-tips>.

⁸⁸ 78 FR 18294.

⁸⁹ 78 FR 18294.

individual commenters expressed a strong preference for the pat-down; many also stated that they always request a pat-down in lieu of AIT screening. Some individual commenters, however, expressed strong opposition and criticism of current pat-down procedures. Some individual commenters expressed their preference to receive a pat-down, but stated that they feel “punished” by TSA staff when requesting the alternative screening measure. Several commenters opined that TSA screeners deliberately make the opt-out unpleasant so that passengers will use the AIT scanners.

Submissions included remarks about the adequacy of information and signs at screening checkpoints about the AIT screening process. For example, multiple commenters stated that TSA currently lists the scanner as optional, in small print on an 11 x 14 inch poster at a crowded checkpoint. Commenters suggested there is a lack of adequate signage informing passengers of the right to opt-out of AIT. One of these individual commenters suggested that, in order to allow passengers adequate time to read about their right to opt-out of AIT, these signs should be posted throughout the security waiting area instead of in the area where passengers are being called forward for screening. A commenter stated that different airports want people to indicate that they are opting out at different times, but passengers have no way of knowing when to opt out. An advocacy group stated that notification of the opt-out option is not large enough and is placed in an area where passengers will not see the notice. A non-profit organization stated that passengers continue to report that signs are not available, even though TSA stated in the NPRM that detailed explanation of AIT procedures is available on its Web site, and signs are posted at checkpoints.

Other individuals and a privacy advocacy group emphasized that the pat-down is not a reasonable alternative. Many individual commenters remarked that when they choose to opt-out of AIT, they are treated with suspicion, public ridicule, hostility, and retaliation (*e.g.*, long and intentional delays) by the screener, and often are unable to monitor their belongings. Other individuals and advocacy groups objected to the manner in which some TSA staff conduct pat-downs, stating they are more invasive and intrusive than necessary to detect weapons or explosives.

Numerous commenters, including a community organization, a non-profit organization, and individual commenters, characterized the pat-

down as groping or sexual assault that involves touching or rubbing of the breasts and genitals of passengers. The pat-downs were referred to as rough, painful, invasive, offensive, intrusive, humiliating, demeaning, and degrading. Some commenters provided anecdotal accounts related to their experiences being screened by TSA. The majority of these comments referred to personal accounts of pat-downs, including statements that the pat-downs were abusive and extended wait times. Other individual commenters stated that because of their negative pat-down experiences, they have cancelled air travel plans. A number of individual commenters stated that in their experience, TSA employees generally treat passengers in a courteous and professional manner.

Commenters also expressed concerns regarding profiling. A few individual commenters, for example, stated that TSA staff intentionally chose young, female travelers for pat-downs at a higher rate than other travelers. Other commenters suggested that TSA staff discriminate against children and elderly women. It was the concern of an individual commenter that an enhanced pat-down of a child can be detrimental to the child's understanding of the appropriateness of an adult touching them. Furthermore, the individual commenter remarked that the separation of the child from their parent for screening results in distress for both the parent and child. Several individuals, a non-profit organization, and an advocacy group expressed concern for children that must undergo touching during pat-downs. Many individuals and an advocacy group also mentioned psychological trauma caused by pat-downs, particularly for rape survivors and victims of sexual abuse. A few individual commenters noted that pat-downs impose unnecessary risks, given that most TSA screeners do not change their gloves often enough to prevent the spread of disease.

TSA Response: TSA allows individuals generally to opt out of AIT screening and undergo a thorough pat-down instead. TSA has no requirement as to when a passenger should indicate that he or she does not wish to undergo AIT screening. Generally, passengers should make their request for a pat-down when they are directed to the AIT and prior to entering the AIT machine. Such requests can also be made earlier in the screening process. While AIT has been used to conduct primary passenger screening since 2009 and millions of passengers are aware of and have been screened by AIT, TSA posts signs to inform passengers that they may opt-out

of AIT screening. TSA places these signs in the checkpoint prior to the AIT machine. Generally, the signs are 11 x 14 inches to avoid impeding the flow of passengers, because the signs are located in an area where passengers walk to enter the AIT unit. However, TSA permits signs that are 22 x 28 inches. TSA appreciates the commenters' input on the placement and font size associated with the signs, and may in the future revise signage practices to make this information even more prominent to passengers.

While commenters wrote that the thoroughness of the pat-down is inappropriate, it would not make sense to allow passengers to opt out of AIT unless the alternative has similar ability to detect both metallic and non-metallic threat items. The pat-downs are tailored to address the known threat posed by concealed metallic or non-metallic explosives or other weapons, including those concealed on culturally sensitive areas of the body in order to evade detection. The court in the *Corbett* decision upheld the constitutionality of the pat-down. “The pat-downs also promote the governmental interest in airport security because security officers physically touch most areas of passengers' bodies Undeniably, a full-body pat-down intrudes on privacy, but the security threat outweighs that invasion of privacy.”⁹⁰ The court noted that TSA's procedures when conducting a pat-down reduce the invasion of privacy.⁹¹

The pat-down procedures are described on TSA's Web site.⁹² A pat-down is performed if a passenger cannot undergo WTMD or opts out of AIT screening. A pat-down is also performed to resolve alarms or anomalies. A less invasive pat-down may be performed on a random basis. TSA advises individuals entering the checkpoint to divest all items on their person and in their pockets to reduce the likelihood that an alarm will occur. A pat-down is conducted by a TSO of the same gender as the passenger. A passenger may request that the pat-down be performed in private. During a private screening, another TSA employee will always be present and a companion of his or her choosing may accompany the passenger. In addition, the passenger is permitted to bring his carry-on baggage to the location where the pat-down will take place, including any private screening area. A passenger may ask for a chair if he or she needs to sit down. Ordinarily

⁹⁰ *Corbett*, 767 F. 3d at 1182.

⁹¹ *Id.*

⁹² <https://www.tsa.gov/travel/frequently-asked-questions>.